A BELDEN BRAND

User Manual

Redundancy Configuration
MICE Switch Power (MSP)

UM RedundConfig MSP
Release 2.0 02/2013

Technical Support
https://hirschmann-support.belden.eu.com

The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Hirschmann Automation and Control GmbH according to the best of the company's knowledge. Hirschmann reserves the right to change the contents of this document without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the information in this document.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

You can get the latest version of this manual on the Internet at the Hirschmann product site (www.hirschmann.com).

Printed in Germany
Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany
Tel.: +49 1805 141538

Rel. 2.0 - 02/2013 – 11.02.2013

Contents

About this Manual

The “GUI” reference manual contains detailed information on using the graphical interface to operate the individual functions of the device.

The “Command Line Interface” reference manual contains detailed information on using the Command Line Interface to operate the individual functions of the device.

The “Installation” user manual contains a device description, safety instructions, a description of the display, and the other information that you need to install the device.

The “Basic Configuration” user manual contains the information you need to start operating the device. It takes you step by step from the first startup operation through to the basic settings for operation in your environment.

The “Redundancy Configuration” user manual document contains the information you require to select the suitable redundancy procedure and configure it.

The “HiView” user manual contains information for using the HiView GUI application. This application allows you to use the graphical user interface of Hirschmann devices with management independently of other applications, such as a browser.

The Industrial HiVision Network Management Software provides you with additional options for smooth configuration and monitoring:

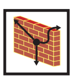
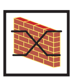
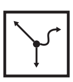
- Simultaneous configuration of multiple devices
- Graphical user interface with network layout
- Auto-topology discovery
- Event log
- Event handling
- Client/server structure
- Browser interface
- ActiveX control for SCADA integration
- SNMP/OPC gateway.

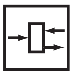
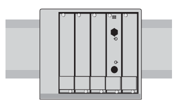
Key

The designations used in this manual have the following meanings:

▶	List
☐	Work step
■	Subheading
Link	Cross-reference with link
Note:	A note emphasizes an important fact or draws your attention to a dependency.
`Courier`	ASCII representation in user interface
	Execution in the Graphical User Interface
	Execution in the Command Line Interface

Symbols used:

	WLAN access point
	Router with firewall
	Switch with firewall
	Router
	Switch

	Bridge
	Hub
	A random computer
	Configuration Computer
	Server
	PLC - Programmable logic controller
	I/O - Robot

1 Network Topology vs. Redundancy Protocols

When using Ethernet, an important prerequisite is that data packets follow a single (unique) path from the sender to the receiver. The following network topologies support this prerequisite:

- Line topology
- Star topology
- Tree topology

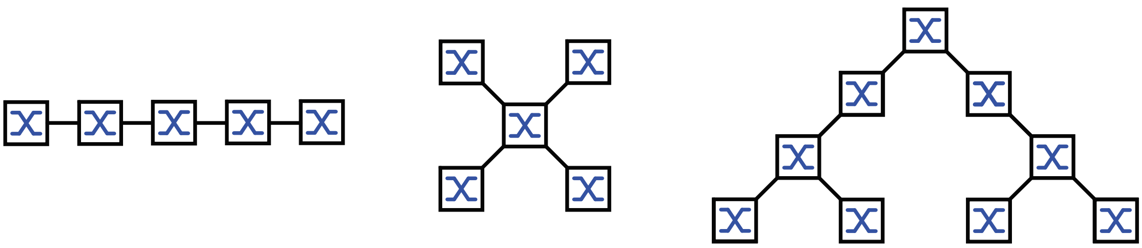


Figure 1: Network with line, star and tree topologies

To ensure that the communication is maintained when a connection fails, you install additional physical connections between the network nodes. Redundancy protocols ensure that the additional connections remain switched off while the original connection is still working. If the connection fails, the redundancy protocol generates a new path from the sender to the receiver via the alternative connection.

To introduce redundancy onto layer 2 of a network, you first define which network topology you require. Depending on the network topology selected, you then choose from the redundancy protocols that can be used with this network topology.

1.1 Network topologies

1.1.1 Meshed topology

For networks with star or tree topologies, redundancy procedures are only possible in connection with physical loop creation. The result is a meshed topology.

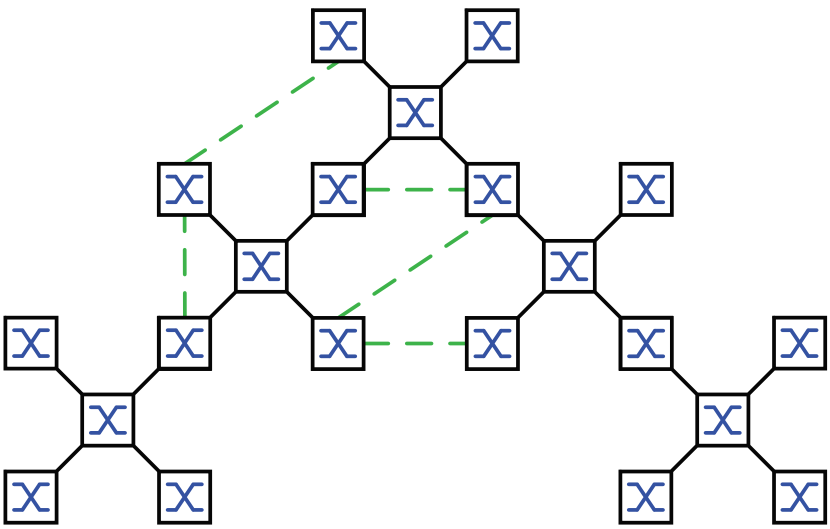


Figure 2: Meshed topology: Tree topology with physical loops

For operating in this network topology, the device provides you with the following redundancy protocols:
- Rapid Spanning Tree (RSTP)

1.1.2 Ring topology

In networks with a line topology, you can use redundancy procedures by connecting the ends of the line. This creates a ring topology.

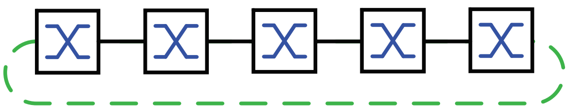


Figure 3: Ring topology: Line topology with connected ends

For operating in this network topology, the device provides you with the following redundancy protocols:
- Media Redundancy Protocol (MRP)
- Rapid Spanning Tree (RSTP)

1.2 Redundancy Protocols

For operating in different network topologies, the device provides you with the following redundancy protocols:

Redundancy protocol	Network topology	Comments
MRP	Ring	The switching time can be selected and is practically independent of the number of devices. An MRP-Ring consits of up to 50 devices that support the MRP protocol according to IEC 62439. If you only use Hirschmann devices, up to 100 devices are possible in the MRP-Ring.
RSTP	Random structure	The switching time depends on the network topology and the number of devices. ▶ typ. < 1 s with RSTP ▶ typ. < 30 s with STP

Table 1: Overview of redundancy protocols

Note: When you are using a redundancy function, you deactivate the flow control on the participating ports. Default setting: flow control deactivated globally and activated on every port.
If the flow control and the redundancy function are active at the same time, the redundancy may not work as intended.

2 Media Redundancy Protocol (MRP)

Since May 2008, the Media Redundancy Protocol (MRP) has been a standardized solution for ring redundancy in the industrial environment.

MRP is compatible with redundant ring coupling, supports VLANs, and is distinguished by very short reconfiguration times.

An MRP-Ring consists of up to 50 devices that support the MRP protocol according to IEC 62439. If you only use Hirschmann devices, up to 100 devices are possible in the MRP-Ring.

2.1 Network Structure

The concept of ring redundancy allows the construction of high-availability, ring-shaped network structures.
With the help of the RM (**R**ing **M**anager) function, the two ends of a backbone in a line structure can be closed to a redundant ring. The ring manager keeps the redundant line open as long as the line structure is intact. If a segment becomes inoperable, the ring manager immediately closes the redundant line, and line structure is intact again.

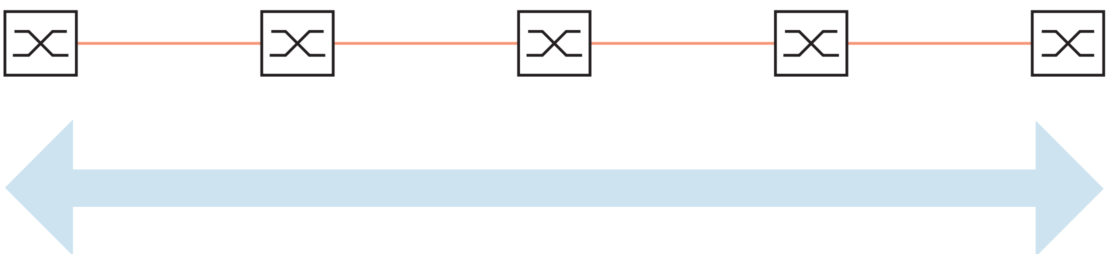


Figure 4: Line structure

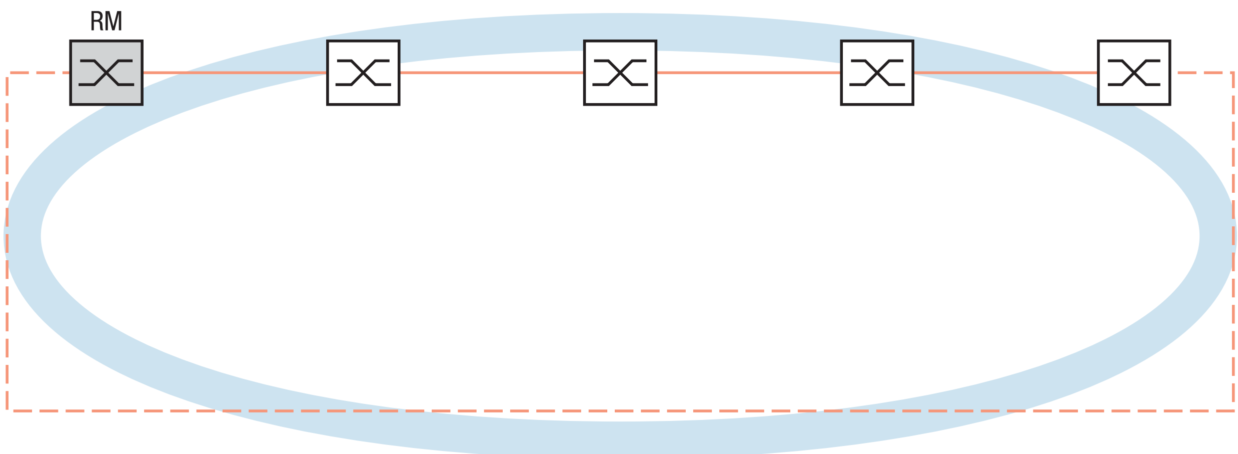


Figure 5: Redundant ring structure
RM = Ring Manager
—— main line
- - - redundant line

2.2 Reconfiguration time

If a line section fails, the ring manager changes the MRP-Ring back into a line structure. You define the maximum time for the reconfiguration of the line in the ring manager.

Possible values for the maximum delay time:
- 500 ms
- 200 ms

Note: You only configure the reconfiguration time with a value less than 500 ms if all the devices in the ring support the shorter delay time.
Otherwise the devices that only support longer delay times might not be reachable due to overloading. Loops can occur as a result.

2.3 Advanced mode

For times even shorter than the guaranteed reconfiguration times, the device provides the advanced mode. The advanced mode speeds up the link failure recognition when the ring participants inform the ring manager of interruptions in the ring via link-down notifications.

Hirschmann devices support link-down notifications. Therefore, you generally activate the advanced mode in the ring manager.

If you are using devices that do not support link-down notifications, the ring manager reconfigures the line in the selected maximum reconfiguration time.

2.4 Prerequisites for MRP

Before setting up an MRP-Ring, make sure that the following conditions are fulfilled:

- All ring participants support MRP.
- The ring participants are connected to each other via the ring ports. Apart from the device’s neighbors, no other ring participants are connected to the respective device.
- All ring participants support the configuration time defined in the ring manager.
- There is exactly 1 ring manager in the ring.

If you are using VLANs, configure every ring port with the following settings:

☐ Deactivate ingress filtering - see the `Switching:VLAN:Port` dialog.

☐ Define the port VLAN ID (PVID) - see the `Switching:VLAN:Port` dialog.
  – PVID = `1` if the device transmits the MRP data packets untagged (VLAN ID = `0` in `Redundancy:MRP` dialog)
  – PVID = `any` if the device transmits the MRP data packets in a VLAN (VLAN ID ≥ `1` in `Redundancy:MRP` dialog)

☐ Define egress rules - see `Switching:VLAN:Static` dialog.
  – `U` (untagged) if the device transmits the MRP data packets untagged (VLAN ID = `0` in `Redundancy:MRP` dialog)
  – `T` (tagged) if the device transmits the MRP data packets in a VLAN (VLAN ID ≥ `1` in `Redundancy:MRP` dialog)

2.5 Example Configuration

A backbone network contains 3 devices in a line structure. To increase the availability of the network, you convert the line structure to a redundant ring structure. Devices from different manufacturers are used.All devices support MRP. On every device you define ports 1.1 and 1.2 as ring ports.

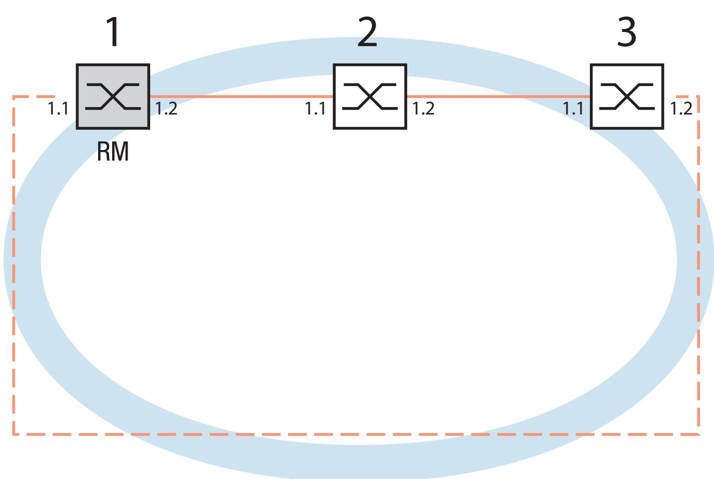


Figure 6: Example of MRP-Ring
RM = Ring Manager
—— main line
- - - redundant line

The following example configuration describes the configuration of the ring manager device (1). You configure the 2 other devices (2 to 3) in the same way, but without activating the ring manager function. This example does not use a VLAN. You have entered 200 ms as the ring recovery time, and all the devices support the advanced mode of the ring manager.

☐ Set up the network to meet your demands.
☐ Configure all ports so that the transmission speed and the duplex settings of the lines correspond to the following table:

Port type	Bit rate	Autonegotiation (automatic configuration)	Port setting	Duplex
TX	100 Mbit/s	off	on	100 Mbit/s full duplex (FDX)
TX	1 Gbit/s	on	on	-
Optical	100 Mbit/s	off	on	100 Mbit/s full duplex (FDX)
Optical	1 Gbit/s	on	on	-

Table 2: Port settings for ring ports

Note: You configure optical ports without support for autonegotiation (automatic configuration) with 100 Mbit/s full duplex (FDX) or 1000 Mbit/s full duplex (FDX).

Note: Configure all the devices of the MRP-Ring individually. Before you connect the redundant line, you must have completed the configuration of all the devices of the MRP-Ring. You thus avoid loops during the configuration phase.

☐ You deactivate the flow control on the participating ports.
If the flow control and the redundancy function are active at the same time, there is a risk that the redundancy function will not operate as intended. (Default setting: flow control deactivated globally and activated on all ports.)

☐ Switch Spanning Tree off on all devices in the network:

☐ Open the `Redundancy:Spanning Tree:Global` dialog.

☐ Switch off the function.
In the state on delivery, Spanning Tree is switched on on the device.

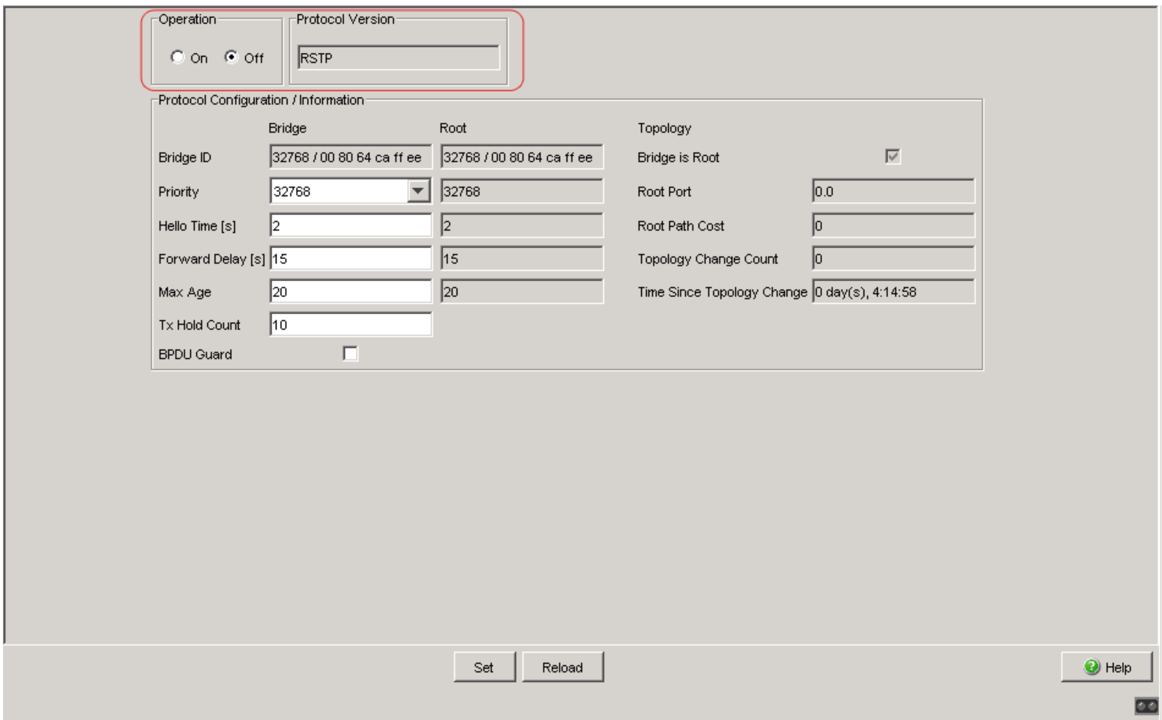


Figure 7: Switching the function off

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`no spanning-tree operation`	Switches Spanning Tree off.
`show spanning-tree global`	Displays the parameters for checking.

☐ Switch MRP on on all devices in the network:

☐ Open the `Redundancy:MRP` dialog.

☐ Define the desired ring ports.

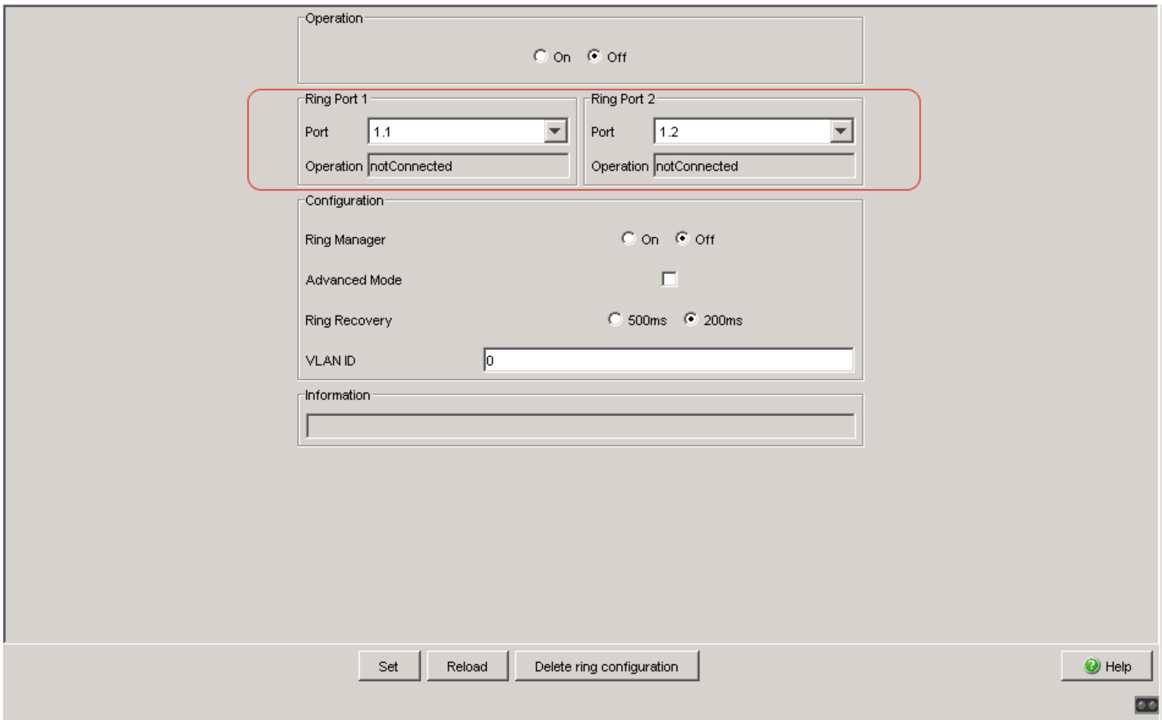


Figure 8: Defining the ring ports

In the Command Line Interface you first define an additional parameter, the MRP domain ID. Configure all the ring participants with the same MRP domain ID. The MRP domain ID is a sequence of 16 number blocks (8-bit values).

When configuring with the graphical user interface, the device uses the default value `255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255`.

`mrp domain add default-domain`	Creates a new MRP domain with the default domain ID.
`mrp domain modify port primary 1/1`	Defines port 1.1 as ring port 1 (primary).
`mrp domain modify port secondary 1/2`	Defines port 1.2 as ring port 2 (secondary).

☐ Activate the ring manager.
For the other devices in the ring, leave the setting as `Off`.

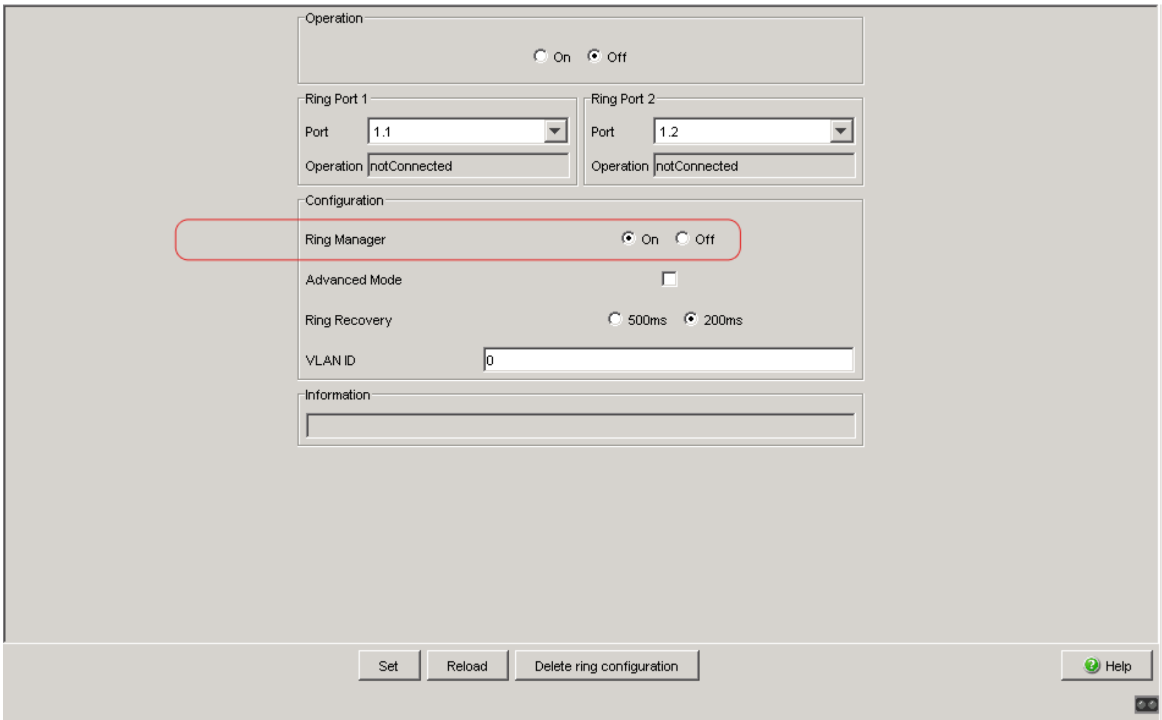


Figure 9: Activating the ring manager

`mrp domain modify mode manager`	Defines the device as the ring manager. Do not activate the ring manager on any other device.

☐ Select the checkbox in the "Advanced Mode" field.

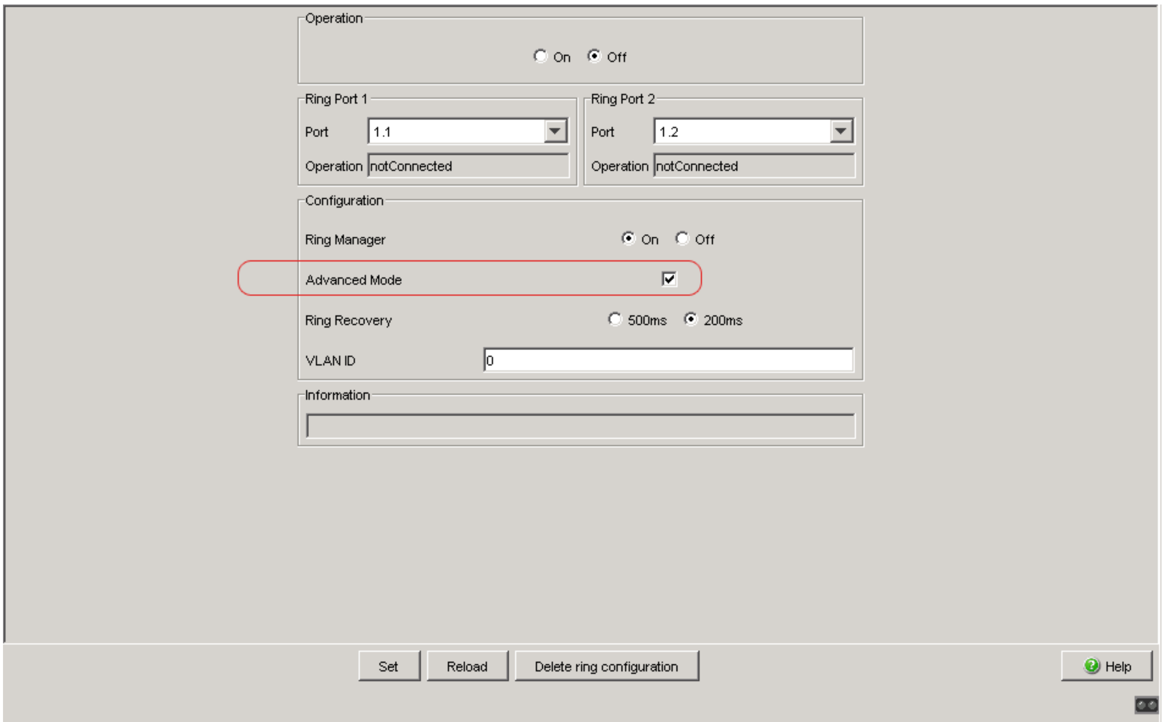


Figure 10: Activating the advanced mode

`mrp domain modify advanced-mode enabled`	Activates the advanced mode.

☐ In the "Ring Recovery" field, select the value `200ms`.

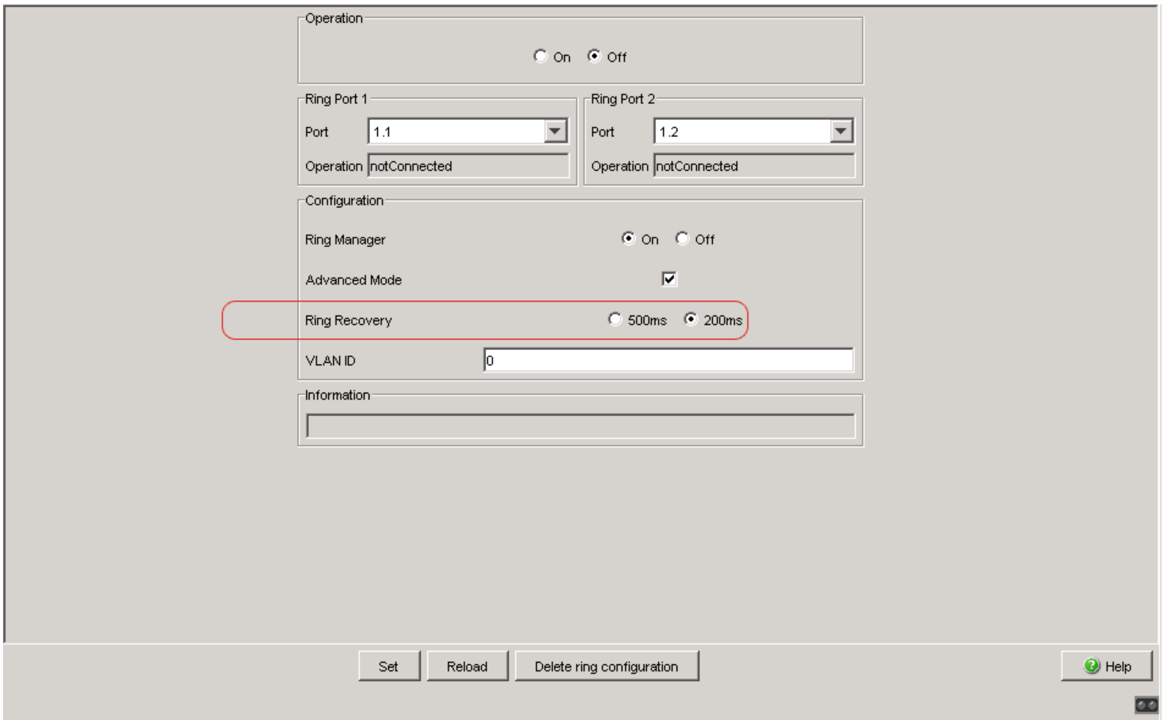


Figure 11: Defining the time for the ring recovery

`mrp domain modify recovery-delay 200ms`	Defines `200ms` as the max. delay time for the reconfiguration of the ring.

Note: If selecting 200 ms for the ring recovery does not provide the ring stability necessary to meet the requirements of your network, you select 500 ms.

☐ Leave the value in the "VLAN" field as `0`.

☐ Switch the operation of the MRP-Ring on.

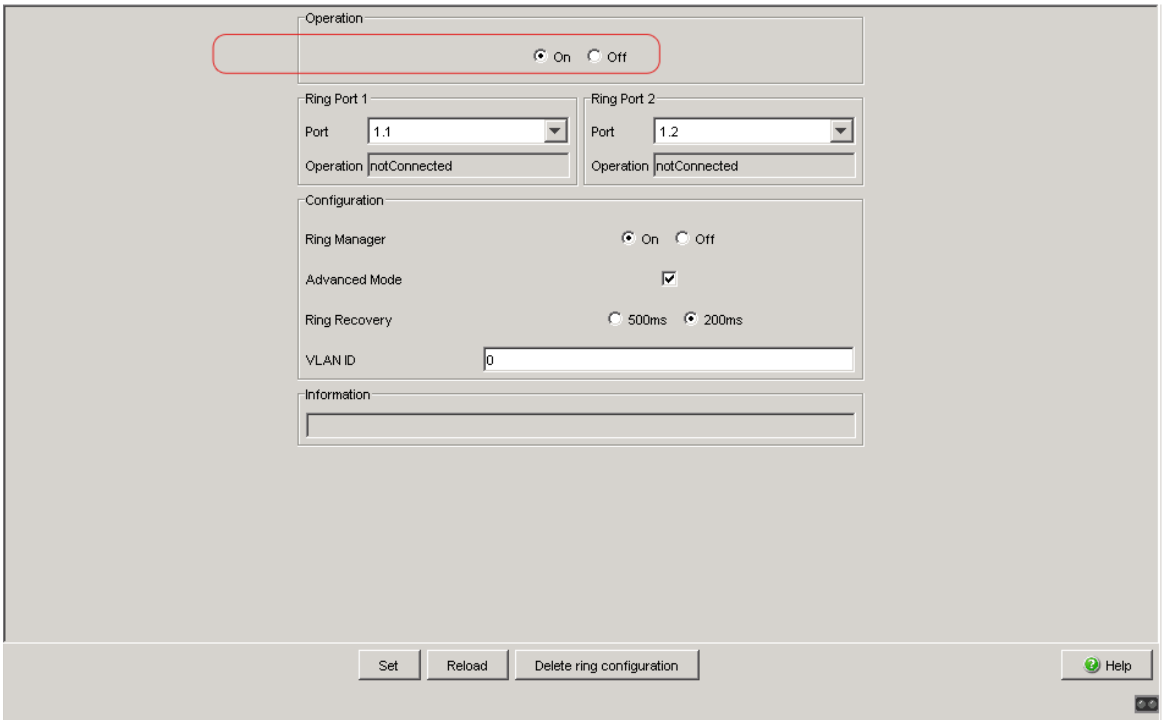


Figure 12: Switching on the MRP function

☐ Click on “Set” to save the changes.

`mrp domain modify operation enable`	Activates the MRP-Ring.

☐ When all the ring participants are configured, close the line to the ring. To do this, you connect the devices at the ends of the line via their ring ports.

☐ Check the messages from the device:

`show mrp`	Displays the parameters for checking.

The "Operation" field shows the operating state of the ring port.

Possible values:

- `forwarding`
  Port is switched on, connection exists.
- `blocked`
  Port is blocked, connection exists.
- `disabled`
  Port is disabled.
- `not connected`
  No connection exists.

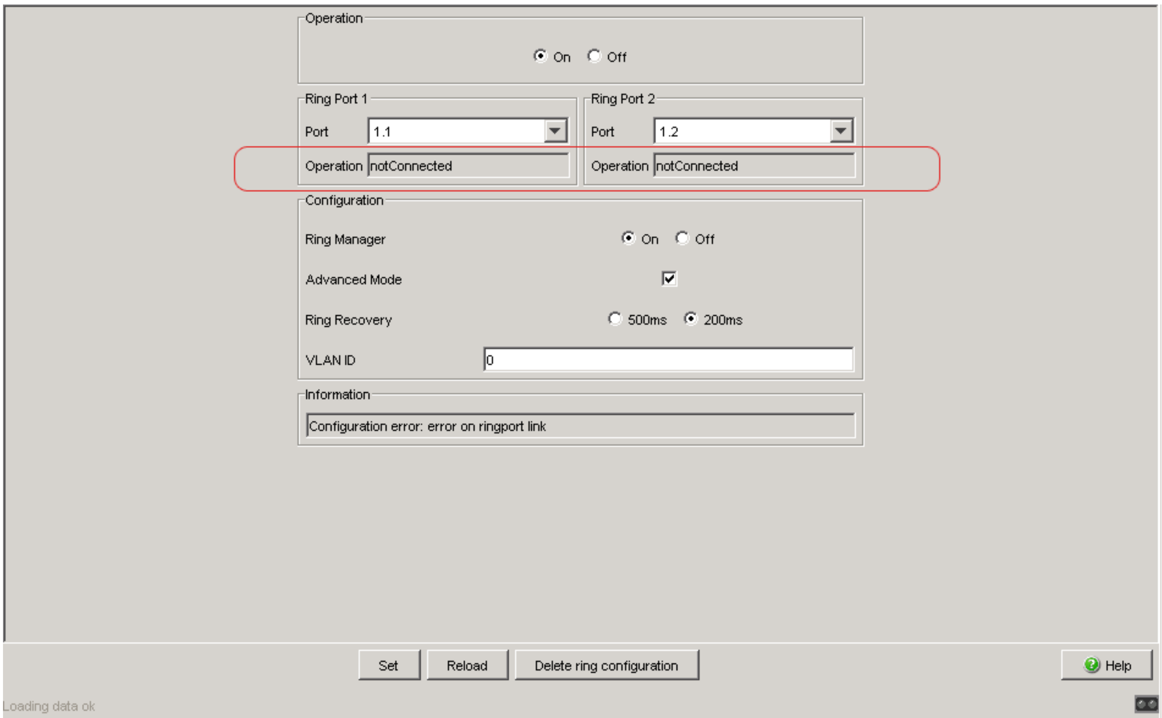


Figure 13: Messages in the "Operation" field

The "Information" field shows messages for the redundancy configuration and the possible causes of errors.

The following messages are possible if the device is operating as a ring client or a ring manager:

- `Redundancy Available`
  The redundancy is set up. When a component of the ring is down, the redundant line takes over its function.
- `Configuration error: Ring port link error`
  Error in the cabling of the ring ports.

The following messages are possible if the device is operating as a ring manager:

- `Configuration error: Packet of other ring manager received`
  Another device exists in the ring that is operating as the ring manager.
  Activate the "Ring Manager" function if there is exactly one device in the ring.
- `Configuration error: Connection in ring is connected to incorrect port`
  A line in the ring is connected with a different port instead of with a ring port. The device only receives test data packets on 1 ring port.

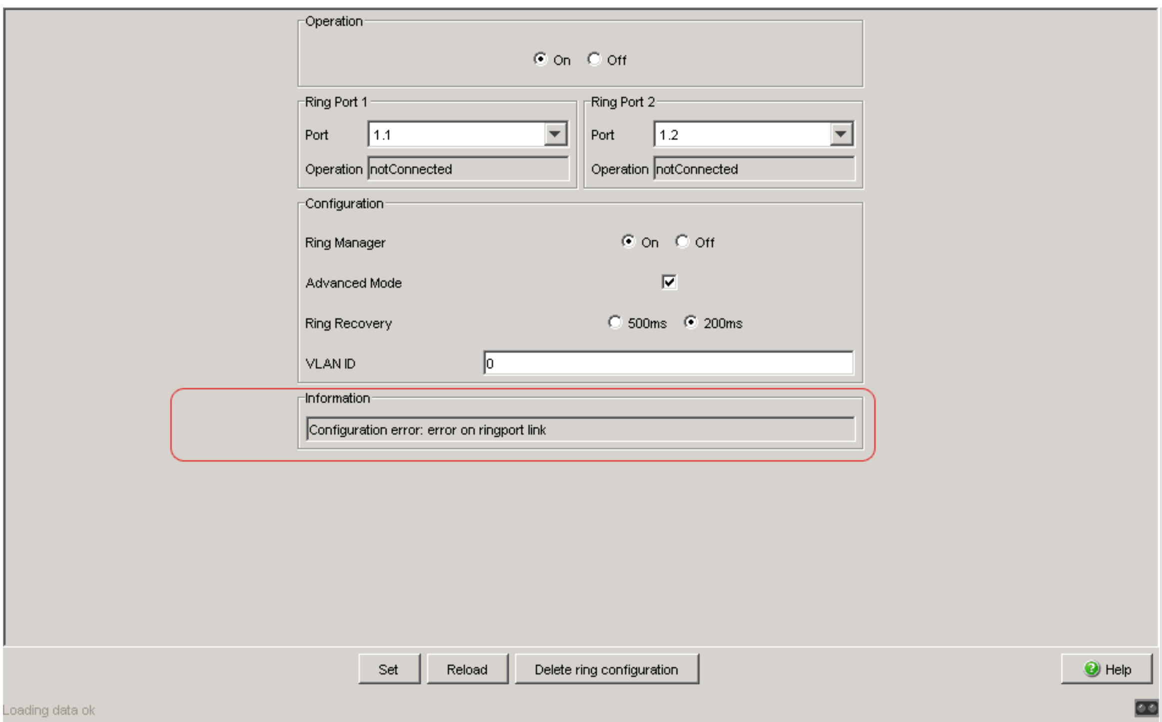


Figure 14: Messages in the "Information" field

☐ If applicable, integrate the MRP ring into a VLAN:

☐ Change the value in the "VLAN" field.

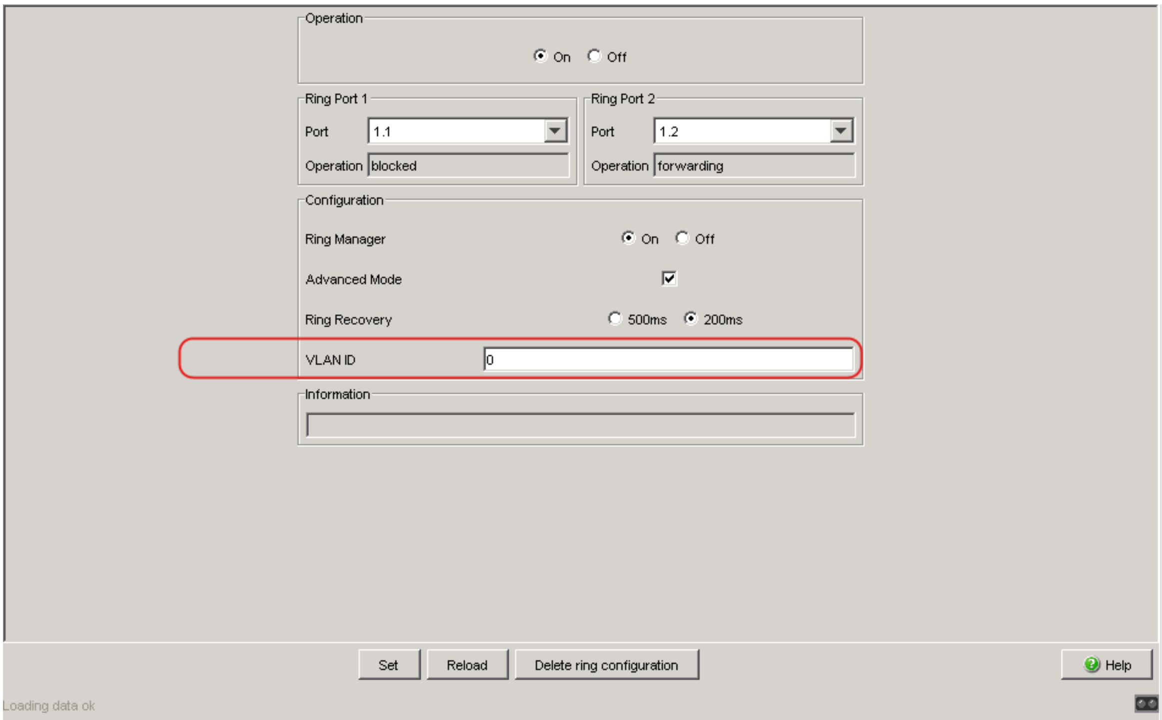


Figure 15: Changing the VLAN ID

- If the MRP-Ring is not assigned to a VLAN (link in this example), leave the VLAN ID as `0`.
  In the `Switching:VLAN:Static` dialog, define the VLAN membership as `U` (untagged) for the ring ports in VLAN `1`.
- If the MRP-Ring is assigned to a VLAN, enter a VLAN ID >`0`.
  In the `Switching:VLAN:Static` dialog, define the VLAN membership as `T` (tagged) for the ring ports in the selected VLAN.

`mrp domain modify vlan <0..4042>`	Assigns the VLAN ID ...

3 Spanning Tree

Note: The Spanning Tree Protocol is a protocol for MAC bridges. For this reason, the following description uses the term bridge for Switch.

Local networks are getting bigger and bigger. This applies to both the geographical expansion and the number of network participants. Therefore, it is advantageous to use multiple bridges, for example:

- to reduce the network load in sub-areas,
- to set up redundant connections and
- to overcome distance limitations.

However, using multiple bridges with multiple redundant connections between the subnetworks can lead to loops and thus loss of communication across of the network. In order to help avoid this, you can use Spanning Tree. Spanning Tree enables loop-free switching through the systematic deactivation of redundant connections. Redundancy enables the systematic reactivation of individual connections as needed.

RSTP is a further development of the Spanning Tree Protocol (STP) and is compatible with it. If a connection or a bridge becomes inoperable, the STP required a maximum of 30 seconds to reconfigure. This is no longer acceptable in time-sensitive applications. RSTP achieves average reconfiguration times of less than a second. When you use RSTP in a ring topology with 10 to 20 devices, you can even achieve reconfiguration times in the order of milliseconds.

Note: RSTP reduces a layer 2 network topology with redundant paths into a tree structure (Spanning Tree) that does not contain any more redundant paths. One of the Switches takes over the role of the root bridge here. The maximum number of devices permitted in an active branch (from the root bridge to the tip of the branch) is specified by the variable `Max Age` for the current root bridge. The preset value for `Max Age` is 20, which can be increased up to 40.

If the device working as the root is inoperable and another device takes over its function, the `Max Age` setting of the new root bridge determines the maximum number of devices allowed in a branch.

Note: The RSTP standard dictates that all the devices within a network work with the (Rapid) Spanning Tree Algorithm. If STP and RSTP are used at the same time, the advantages of faster reconfiguration with RSTP are lost in the network segments that are operated in combination.
A device that only supports RSTP works together with MSTP devices by not assigning an MST region to itself, but rather the CST (Common Spanning Tree).

3.1 Basics

Because RSTP is a further development of the STP, all the following descriptions of the STP also apply to the RSTP.

3.1.1 The tasks of the STP

The Spanning Tree Algorithm reduces network topologies built with bridges and containing ring structures due to redundant links to a tree structure. In doing so, STP opens ring structures according to preset rules by deactivating redundant paths. If a path is interrupted because a network component becomes inoperable, STP reactivates the previously deactivated path again. This allows redundant links to increase the availabiliy of communication. STP determines a bridge that represents the STP tree structure‘s base. This bridge is called root bridge.

Features of the STP algorithm:

- automatic reconfiguration of the tree structure in the case of a bridge becoming inoperable or the interruption of a data path
- the tree structure is stabilized up to the maximum network size,
- stabilization of the topology within a short time period
- topology can be specified and reproduced by the administrator
- transparency for the terminal devices
- low network load relative to the available transmission capacity due to the tree structure created

3.1.2 Bridge parameters

In the context of Spanning Treee, each bridge and its connections are uniquely described by the following parameters:

- Bridge Identifier
- Root Path Cost for the bridge ports,
- Port Identifier

3.1.3 Bridge Identifier

The Bridge Identifier consists of 8 bytes. The 2 highest-value bytes are the priority. The default setting for the priority number is 32,768, but the Management Administrator can change this when configuring the network. The 6 lowest-value bytes of the bridge identifier are the bridge's MAC address. The MAC address allows each bridge to have unique bridge identifiers.
The bridge with the smallest number for the bridge identifier has the highest priority.

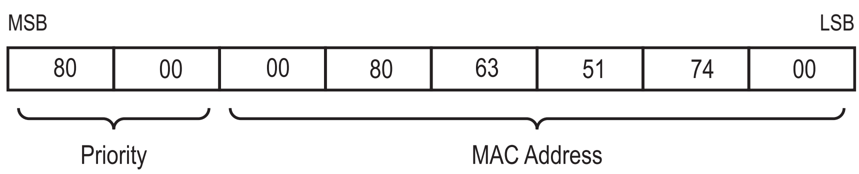


Figure 16: Bridge Identifier, Example (values in hexadecimal notation)

3.1.4 Root Path Cost

Each path that connects 2 bridges is assigned a cost for the transmission (path cost). The Switch determines this value based on the transmission speed (see table 3). It assigns a higher path cost to paths with lower transmission speeds.

Alternatively, the Administrator can set the path cost. Like the Switch, the Administrator assigns a higher path cost to paths with lower transmission speeds. However, since the Administrator can choose this value freely, he has a tool with which he can give a certain path an advantage among redundant paths.

The root path cost is the sum of all individual costs of those paths that a data packet has to traverse from a connected bridge‘s port to the root bridge.

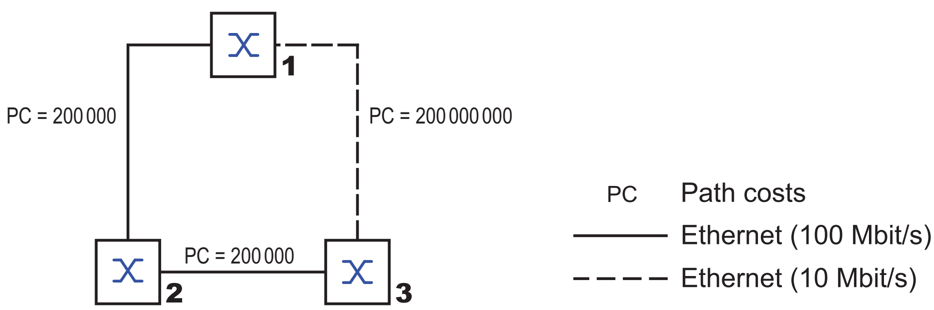


Figure 17: Path costs

Data rate	Recommended value	Recommended range	Possible range
≤100 Kbit/s	200,000,000[a]	20,000,000-200,000,000	1-200,000,000
1 Mbit/s	20,000,000[a]	2,000,000-200,000,000	1-200,000,000
10 Mbit/s	2,000,000[a]	200,000-20,000,000	1-200,000,000
100 Mbit/s	200,000[a]	20,000-2,000,000	1-200,000,000
1 Gbit/s	20,000	2,000-200,000	1-200,000,000
10 Gbit/s	2,000	200-20,000	1-200,000,000
100 Gbit/s	200	20-2,000	1-200,000,000
1 TBit/s	20	2-200	1-200,000,000
10 TBit/s	2	1-20	1-200,000,000

Table 3: Recommended path costs for RSTP based on the data rate.

a. Bridges that conform with IEEE 802.1D 1998 and only support 16-bit values for the path costs should use the value 65,535 (FFFFH) for path costs when they are used in conjunction with bridges that support 32-bit values for the path costs.

3.1.5 Port Identifier

The port identifier consists of 2 bytes. One part, the lower-value byte, contains the physical port number. This provides a unique identifier for the port of this bridge. The second, higher-value part is the port priority, which is specified by the Administrator (default value: 128). It also applies here that the port with the smallest number for the port identifier has the highest priority.

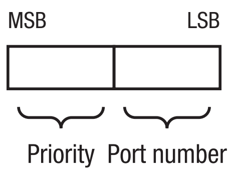


Figure 18: Port Identifier

3.1.6 Max Age and Diameter

The “Max Age” and “Diameter” values largely determine the maximum expansion of a Spanning Tree network.

- **Diameter**

  The number of connections between the devices in the network that are furthest removed from each other is known as the network diameter.

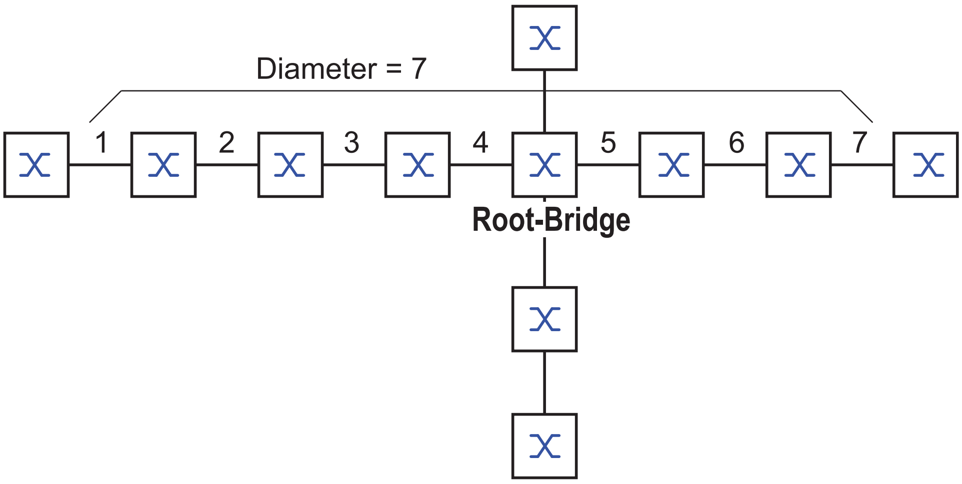


Figure 19: Definition of diameter

The network diameter that can be achieved in the network is MaxAge-1. In the state on delivery, MaxAge=20 and the maximum diameter that can be achieved=19. If you set the maximum value of 40 for MaxAge, the maximum diameter that can be achieved=39.

MaxAge

Every STP-BPDU contains a “MessageAge” counter. When a bridge is passed through, the counter increases by 1.
Before forwarding a STP-BPDU, the bridge compares the “MessageAge” counter with the “MaxAge” value defined in the device:

- ☐ If MessageAge < MaxAge, the bridge forwards the STP-BPDU to the next bridge.
- ☐ If MessageAge = MaxAge, the bridge discards the STP-BPDU.

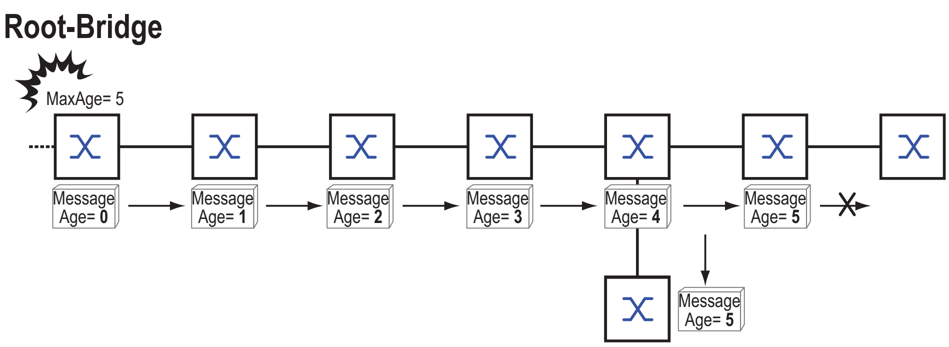


Figure 20: Transmission of an STP-BPDU depending on MaxAge

3.2 Rules for Creating the Tree Structure

3.2.1 Bridge information

To determine the tree structure, the bridges need more detailed information about the other bridges located in the network.
To obtain this information, each bridge sends a BPDU (Bridge Protocol Data Unit) to the other bridges.

The contents of a BPDU include

- bridge identifier,
- root path costs and
- port identifier

(see IEEE 802.1D).

3.2.2 Setting up the tree structure

- The bridge with the smallest number for the bridge identifier is called the root bridge. It is (or will become) the root of the tree structure.
- The structure of the tree depends on the root path costs. Spanning Tree selects the structure so that the path costs between each individual bridge and the root bridge become as small as possible.

- If there are multiple paths with the same root path costs, the bridge further away from the root decides which port it blocks. For this purpose, it uses the bridge identifiers of the bridge closer to the root. The bridge blocks the port that leads to the bridge with the numerically higher ID (a numerically higher ID is the logically worse one). If 2 bridges have the same priority, the bridge with the numerically larger MAC address has the numerically higher ID, which is logically the worse one.
- If multiple paths with the same root path costs lead from one bridge to the same bridge, the bridge further removed from the root uses the port identifier of the other bridge as the last criterion (see fig. 18). In the process, the bridge blocks the port that leads to the port with the numerically higher ID (a numerically higher ID is the logically worse one). If 2 ports have the same priority, the port with the higher port number has the numerically higher ID, which is logically the worse one.

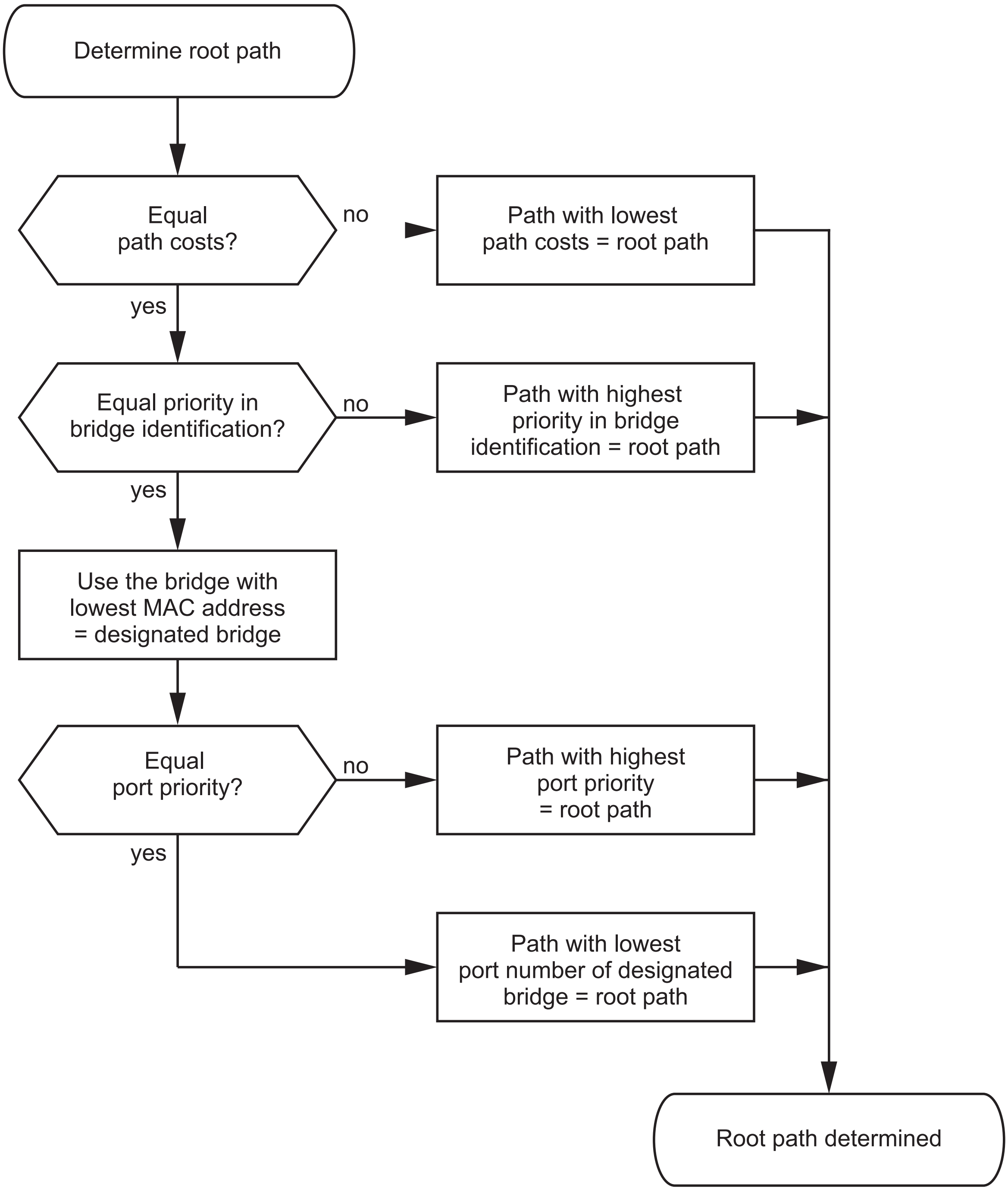


Figure 21: Flow diagram for specifying the root path

3.3 Examples

3.3.1 Example of determining the root path

You can use the network plan (see fig. 22) to follow the flow chart (see fig. 21) for determining the root path. The administrator has specified a priority in the bridge identification for each bridge. The bridge with the smallest numerical value for the bridge identification takes on the role of the root bridge, in this case, bridge 1. In the example all the sub-paths have the same path costs. The protocol blocks the path between bridge 2 and bridge 3 as a connection from bridge 3 via bridge 2 to the root bridge would result in higher path costs.

The path from bridge 6 to the root bridge is interesting:

- The path via bridge 5 and bridge 3 creates the same root path costs as the path via bridge 4 and bridge 2.
- STP selects the path using the bridge that has the lowest MAC address in the bridge identification (bridge 4 in the illustration).
- There are also 2 paths between bridge 6 and bridge 4. The port identifier is decisive here (Port 1 < Port 3).

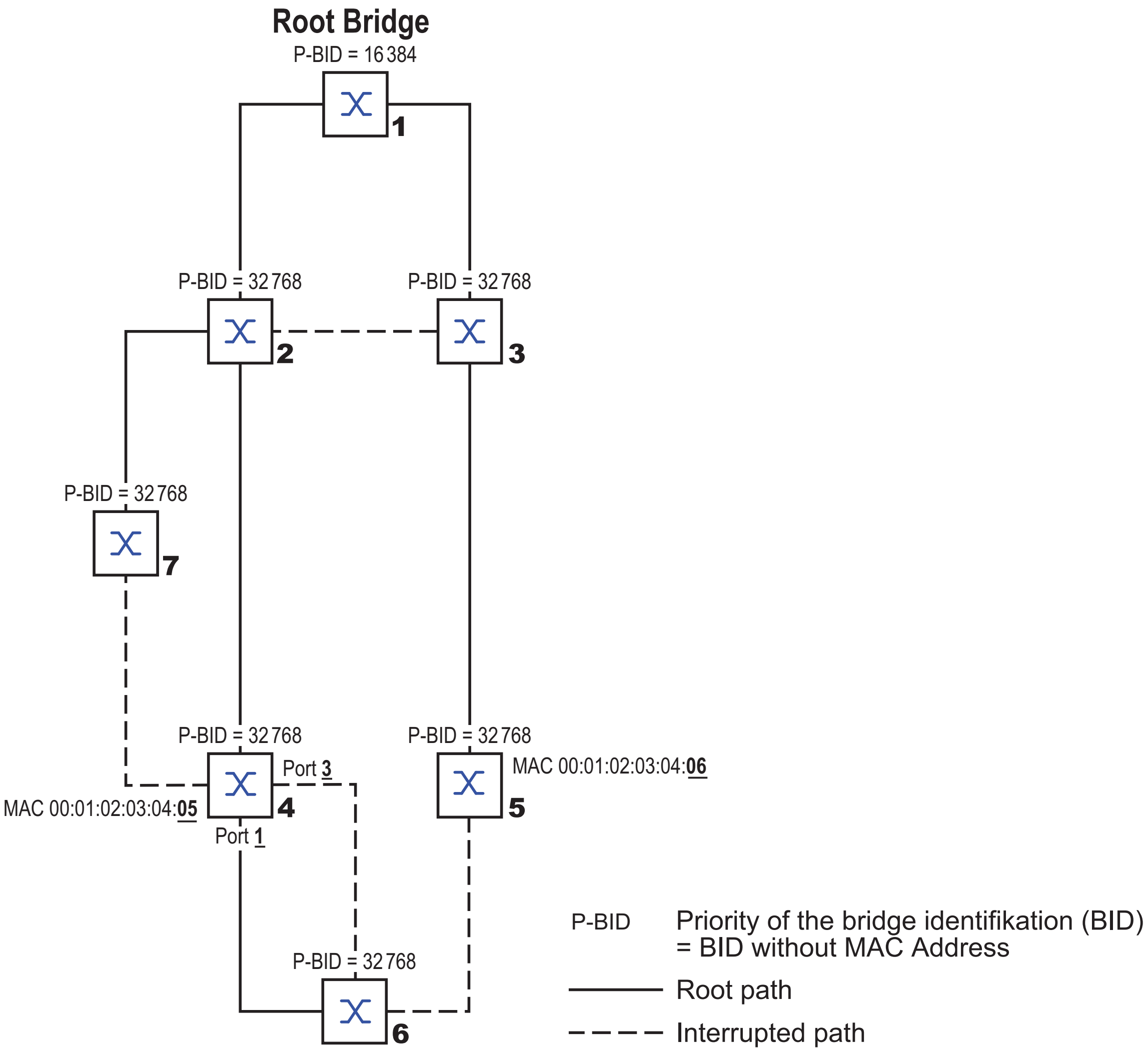


Figure 22: Example of determining the root path

3.3.2 Example of manipulating the root path

You can use the network plan (see fig. 23) to follow the flow chart (see fig. 21) for determining the root path. The Administrator has performed the following:

- Left the default value of 32,768 (8000H) for every bridge apart from bridge 1 and bridge 5, and
- assigned to bridge 1 the value 16,384 (4000H), thus making it the root bridge.
- To bridge 5 he assigned the value 28,672 (7000H).

In the example, all the sub-paths have the same path costs. The protocol blocks the path between bridge 2 and bridge 3 as a connection from bridge 3 via bridge 2 to the root bridge would mean higher path costs.

The path from bridge 6 to the root bridge is interesting:

- ▶ The path via bridge 5 and bridge 3 creates the same root path costs as the path via bridge 4 and bridge 2.
- ▶ The bridges select the path via bridge 4 because the value 28,672 for the priority in the bridge identifier is smaller than value 32,768.

Note: Because the Administrator does not change the default values for the priorities of the bridges in the bridge identifier, apart from the value for the root bridge, the MAC address in the bridge identifier alone determines which bridge becomes the new root bridge if the current root bridge goes down.

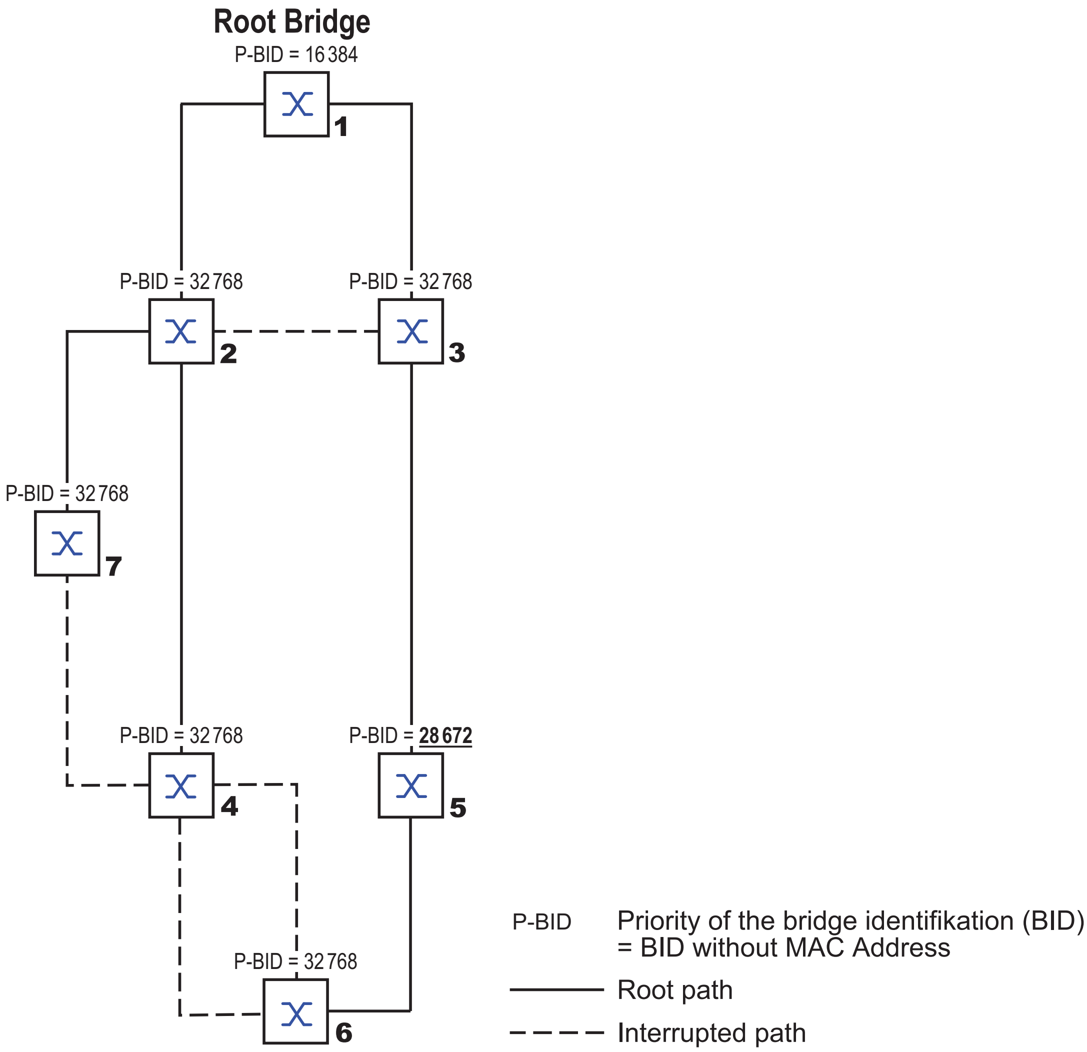


Figure 23: Example of manipulating the root path

3.3.3 Example of manipulating the tree structure

The Management Administrator soon discovers that this configuration with bridge 1 as the root bridge (see on page 40 “Example of determining the root path”) is invalid. On the paths from bridge 1 to bridge 2 and bridge 1 to bridge 3, the control packets which the root bridge sends to all other bridges add up. If the Management Administrator configures bridge 2 as the root bridge, the burden of the control packets on the subnetworks is distributed much more evenly. The result is the configuration shown here (see fig. 24). The path costs for most of the bridges to the root bridge have decreased.

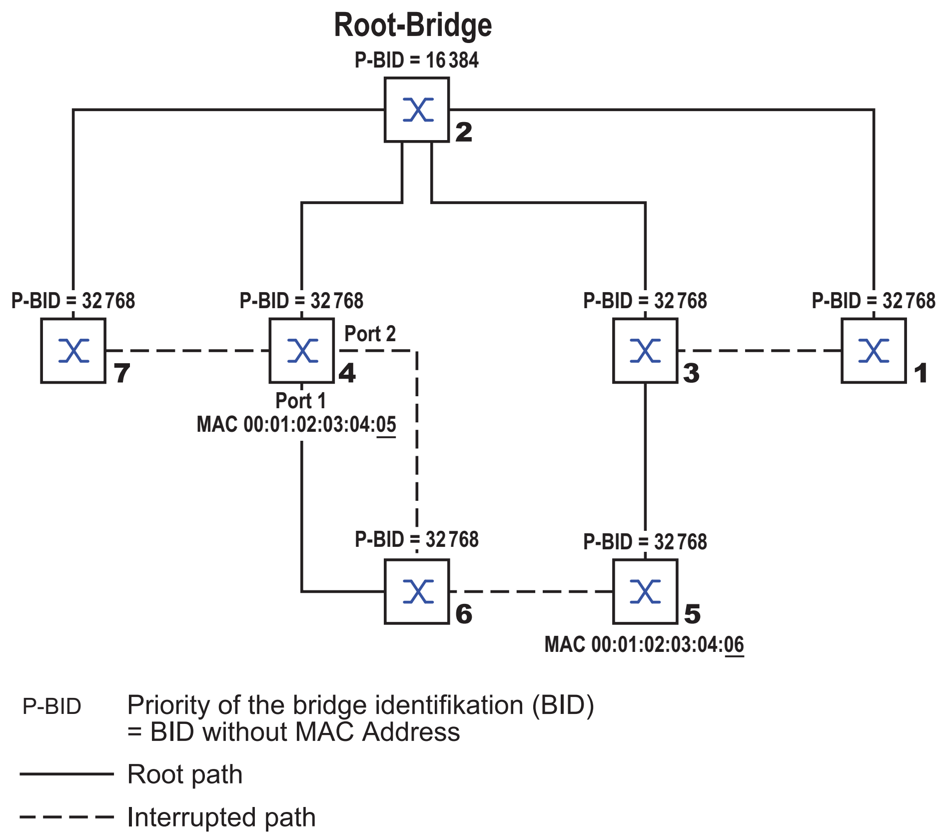


Figure 24: Example of manipulating the tree structure

3.4 The Rapid Spanning Tree Protocol

The RSTP uses the same algorithm for determining the tree structure as STP. RSTP merely changes parameters, and adds new parameters and mechanisms that speed up the reconfiguration if a link or bridge becomes inoperable.
The ports play a significant role in this context.

3.4.1 Port roles

RSTP assigns each bridge port one of the following roles (see fig. 25):

- Root Port:
  This is the port at which a bridge receives data packets with the lowest path costs from the root bridge.
  If there are multiple ports with equally low path costs, the bridge ID of the bridge that leads to the root (designated bridge) decides which of its ports is given the role of the root port by the bridge further removed from the root.
  If a bridge has multiple ports with equally low path costs to the same bridge, the bridge uses the port ID of the bridge leading to the root (designated bridge) to decide which port it selects locally as the root port (see fig. 21).
  The root bridge itself does not have a root port.
- Designated port:
  The bridge in a network segment that has the lowest root path costs is the designated bridge.
  If more than 1 bridge has the same root path costs, the bridge with the smallest value bridge identifier becomes the designated bridge. The port on this bridge that connects it to a network segment leading to the root bridge, is the designated port.

- Edge port
  Every network segment with no additional RSTP bridges is connected with exactly one designated port. In this case, this designated port is also an edge port. The distinction of an edge port is the fact that it does not receive any RST BPDUs (Rapid Spanning Tree Bridge Protocol Data Units).
- Alternate port
  This is a blocked port that takes over the task of the bridge port if the connection to the root bridge is lost. The alternate port provides a backup connection to the root bridge.
- Backup port
  This is a blocked port that serves as a backup in case the connection to the designated port of this network segment (without any RSTP bridges) is lost
- Disabled port
  This is a port that does not participate in the Spanning Tree Operation, i.e., the port is switched off or does not have any connection.

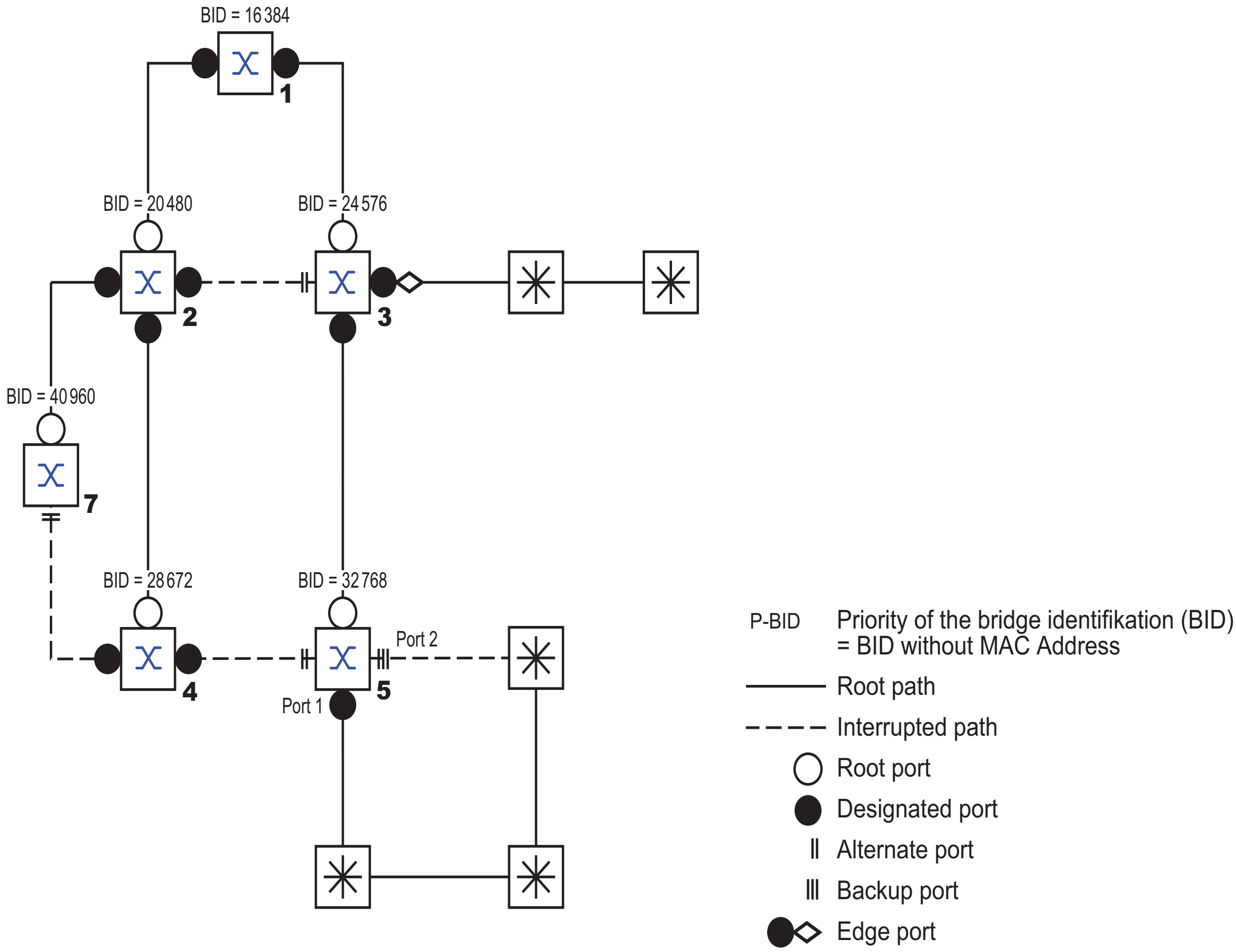


Figure 25: Port role assignment

3.4.2 Port states

Depending on the tree structure and the state of the selected connection paths, the RSTP assigns the ports their states.

STP port state	Administrative bridge port state	MAC operational	RSTP Port state	Active topology (port role)
DISABLED	Disabled	FALSE	Discarding[a]	Excluded (disabled)
DISABLED	Enabled	FALSE	Discarding[a]	Excluded (disabled)
BLOCKING	Enabled	TRUE	Discarding[b]	Excluded (alternate, backup)
LISTENING	Enabled	TRUE	Discarding[b]	Included (root, designated)
LEARNING	Enabled	TRUE	Learning	Included (root, designated)
FORWARDING	Enabled	TRUE	Forwarding	Included (root, designated)

Table 4: Relationship between port state values for STP and RSTP.

a. The dot1d-MIB displays “Disabled”
b. The dot1d-MIB displays “Blocked”

Meaning of the RSTP port states:

- Disabled: Port does not belong to the active topology
- Discarding: No address learning in FDB, no data traffic except for STP BPDUs
- Learning: Address learning active (FDB) and no data traffic except for STP BPDUs
- Forwarding: Address learning is active (FDB), sending and receipt of all frame types (not only STP BPDUs)

3.4.3 Spanning Tree Priority Vector

To assign roles to the ports, the RSTP bridges exchange configuration information with each other. This information is known as the Spanning Tree Priority Vector. It is part of the RSTP BPDUs and contains the following information:

- Bridge identification of the root bridge
- Root path costs of the sending bridge
- Bridge identification of the sending bridge
- Port identifiers of the ports through which the message was sent
- Port identifiers of the ports through which the message was received

Based on this information, the bridges participating in RSTP are able to determine port roles themselves and define the port states of their own ports.

3.4.4 Fast reconfiguration

Why can RSTP react faster than STP to an interruption of the root path?

- Introduction of edge-ports:
  During a reconfiguration, RSTP switches an edge port into the transmission mode after three seconds (default setting) and then waits for the “Hello Time” to elapse, to be sure that no bridge sending BPDUs is connected.
  When the user ensures that a terminal device is connected at this port and will remain connected, there are no waiting times at this port in the case of a reconfiguration.
- Introduction of alternate ports:
  As the port roles are already distributed in normal operation, a bridge can immediately switch from the root port to the alternate port after the connection to the root bridge is lost.
- Communication with neighboring bridges (point-to-point connections):
  Decentralized, direct communication between neighboring bridges enables reaction without wait periods to status changes in the spanning tree topology.

- Address table:
  With STP, the age of the entries in the FDB determines the updating of communication. RSTP immediately deletes the entries in those ports affected by a reconfiguration.
- Reaction to events:
  Without having to adhere to any time specifications, RSTP immediately reacts to events such as connection interruptions, connection reinstatements, etc.

Note: The downside of this fast reconfiguration is the possibility that data packages could be duplicated and/or arrive at the recipient in the wrong order during the reconfiguration phase of the RSTP topology. If this is unacceptable for your application, use the slower Spanning Tree Protocol or select one of the other, faster redundancy procedures described in this manual.

3.4.5 STP compatibility mode

The STP compatibility mode allows you to operate RSTP devices in networks with old installations. If an RSTP device detects an older STP device, it switches on the STP compatibility mode at the relevant port.

3.5 Configuring the device

RSTP configures the network topology completely independently. The device with the lowest bridge priority automatically becomes the root bridge. However, to define a specific network structure regardless, you specify a device as the root bridge. In general, a device in the backbone takes on this role.

☐ Set up the network to meet your requirements, initially without redundant lines.

☐ You deactivate the flow control on the participating ports.
If the flow control and the redundancy function are active at the same time, there is a risk that the redundancy function will not operate as intended. (Default setting: flow control deactivated globally and activated on all ports.)

☐ Switch MRP off on all devices.

☐ Switch Spanning Tree on on all devices in the network.
In the state on delivery, Spanning Tree is switched on on the device.

☐ Open the `Redundancy:Spanning Tree:Global` dialog.

☐ Activate the function.

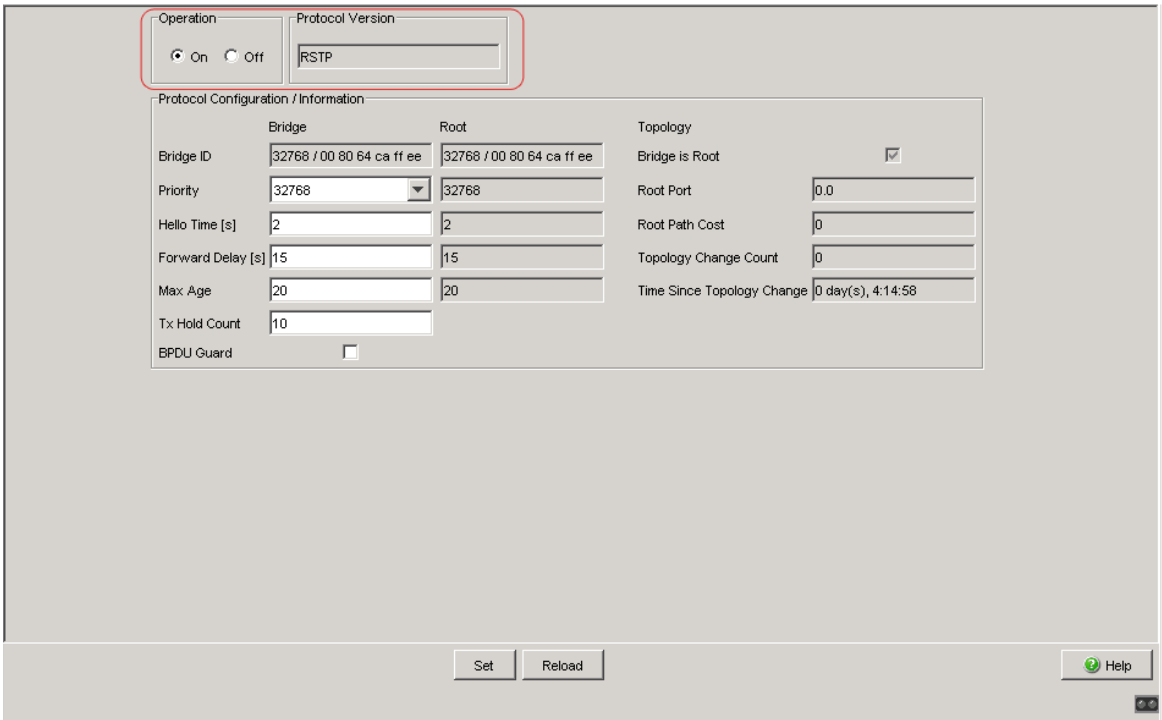


Figure 26: Switching the function on

☐ Click on "Set" to save the changes.

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`spanning-tree operation`	Switches Spanning Tree on.
`show spanning-tree global`	Displays the parameters for checking.

☐ Now connect the redundant lines.

☐ Define the settings for the device that takes over the role of the root bridge.

☐ In the "Priority" field you enter a numerically lower value.
The root bridge receives the numerically lowest bridge priority of all the devices in the network.

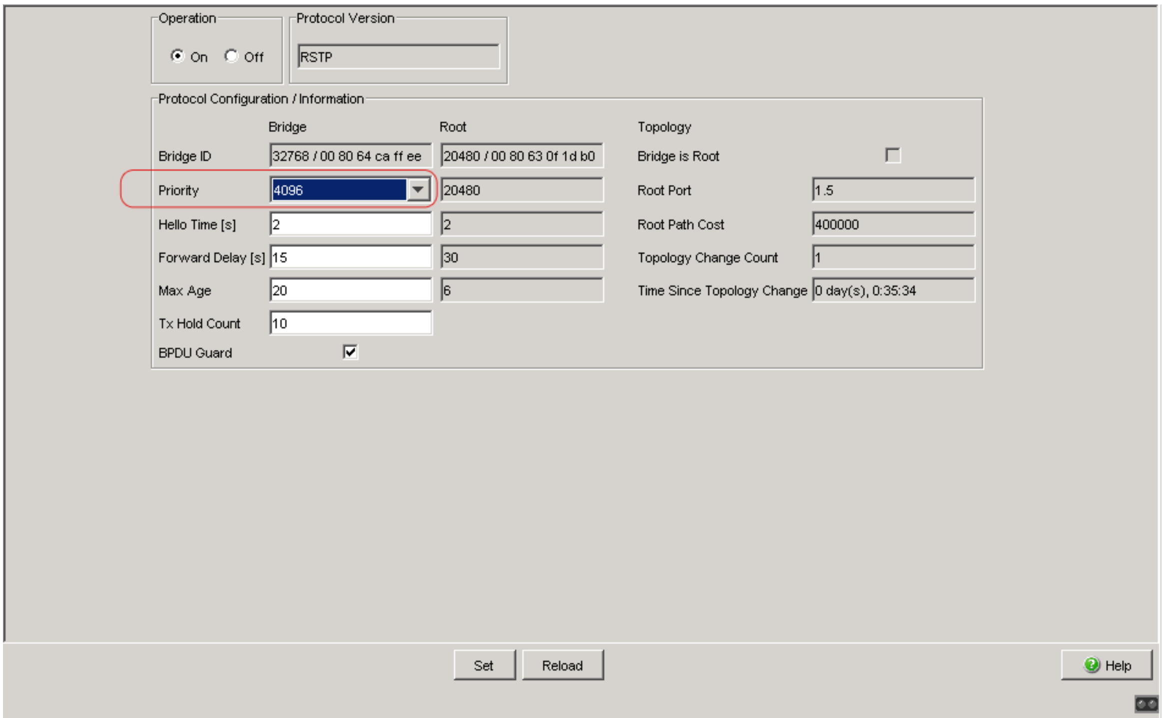


Figure 27: Defining the bridge priority

☐ Click on "Set" to save the changes.

`spanning-tree mst priority 0 <0..61440 in 4096er-Schritten>`	Defines the bridge priority of the device.

After saving, the dialog shows the following information:
- The "Bridge is Root" checkbox is selected.
- The "Root Port" field shows the value `0.0`.
- The "Root Path Cost" field shows the value `0`.

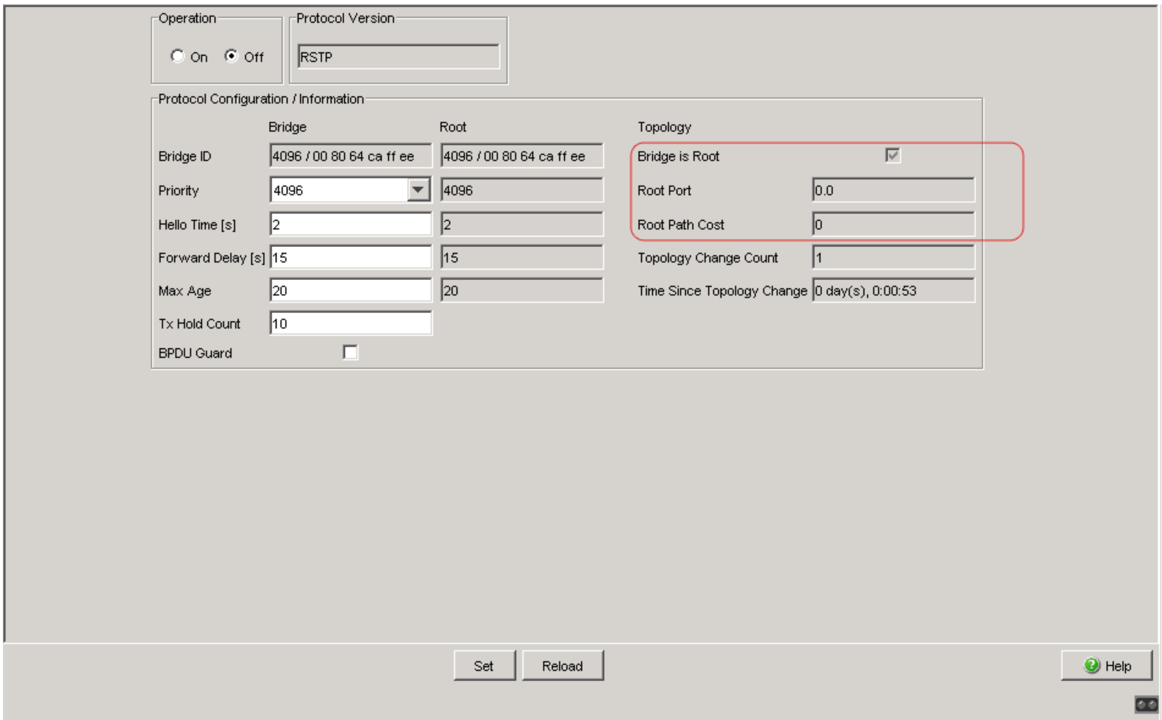


Figure 28: Device is operating as root bridge

`show spanning-tree global`	Displays the parameters for checking.

☐ If applicable, change the values in the "Forward Delay" and "Max Age" fields.

– The root bridge transmits the changed values to the other devices.

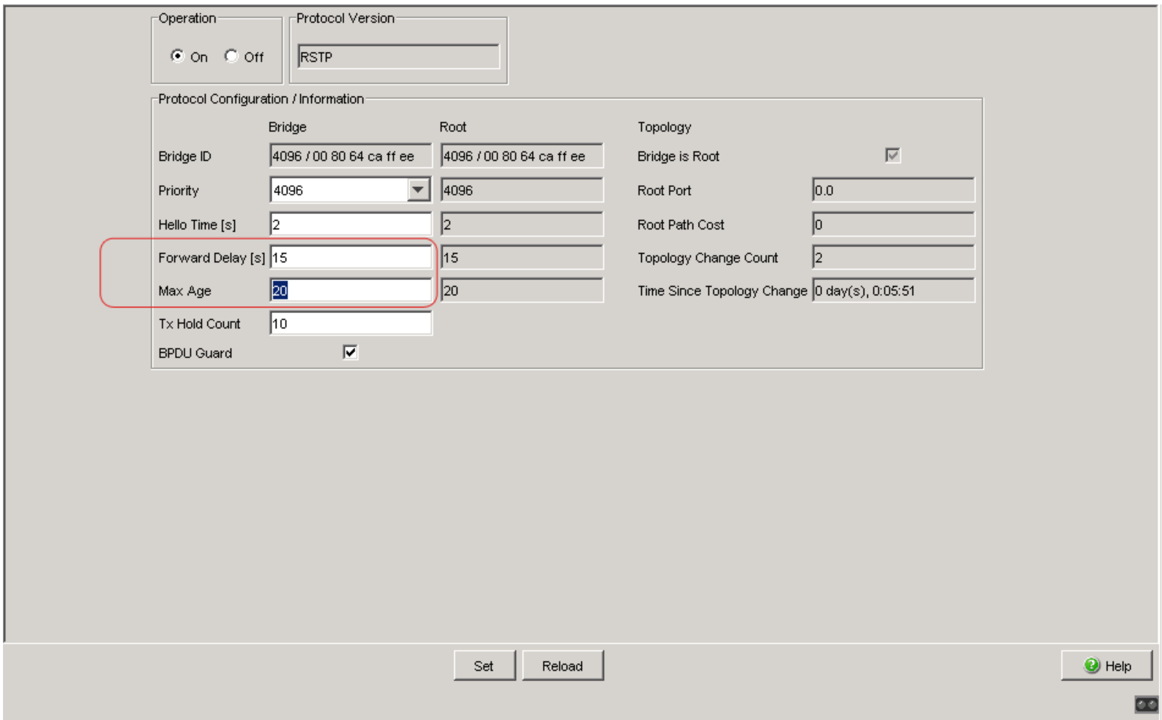


Figure 29: Changing Forward Delay and Max Age

☐ Click on "Set" to save the changes.

`spanning-tree forward-time <4..30>`	Defines the delay time for the status change in seconds.
`spanning-tree max-age <6..40>`	Specifies the maximum permissible branch length, i.e. the number of devices to the root bridge.
`show spanning-tree global`	Displays the parameters for checking.

Note: The parameters "Forward Delay" and "Max Age" have the following relationship:
`Forward Delay` ≥ (`Max Age`/2) + 1
If you enter values in the fields that contradict this relationship, the device replaces these values with the last valid values or with the default value.

Note: If possible, do not change the value in the “Hello Time” field.

☐ Check the following values in the other devices:
- Bridge ID (bridge priority and MAC address) of the corresponding device and the root bridge.
- Number of the device port that leads to the root bridge.
- Path cost from the root port of the device to the root bridge.

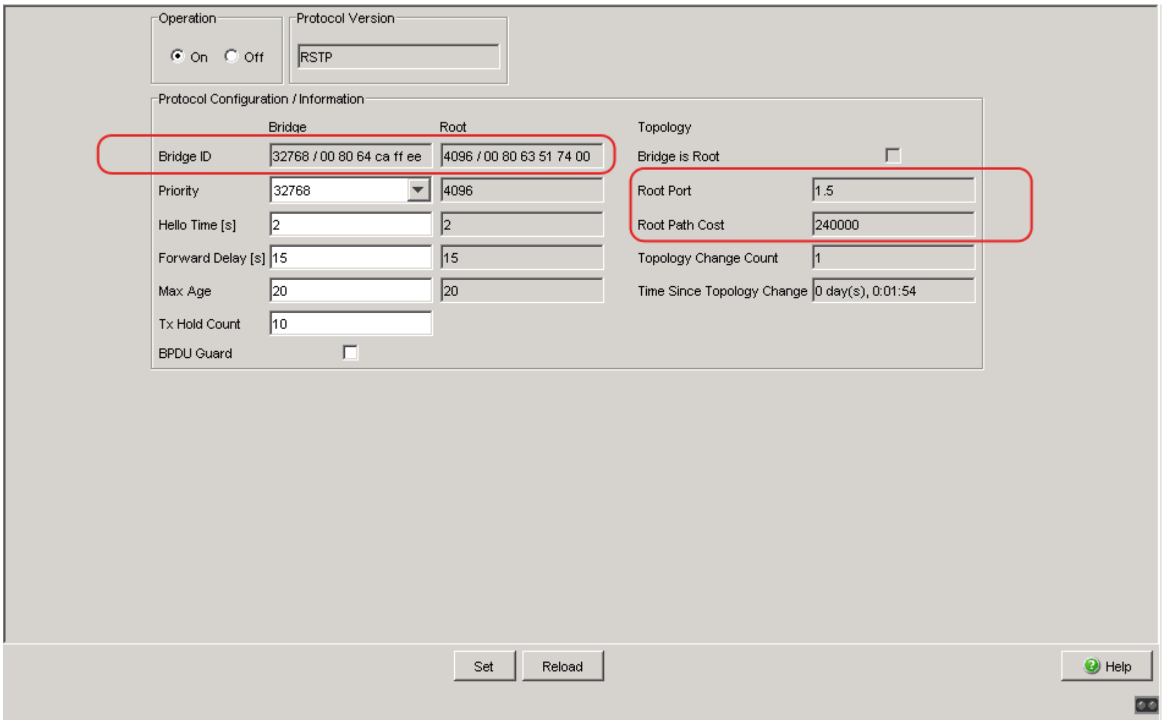


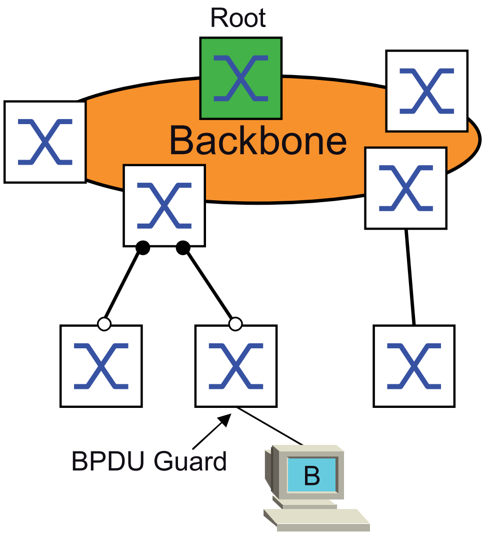
Figure 30: Check values

`show spanning-tree global`	Displays the parameters for checking.

3.6 Guards

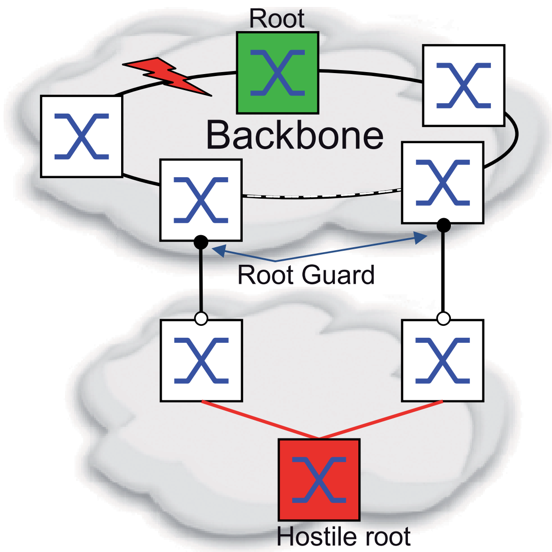
The device allows you to activate various protection functions (guards) on the device ports.
The following protection functions help protect your network from incorrect configurations, loops and attacks with STP-BPDUs:

- BPDU Guard – for manually defined terminal device ports (edge ports)
  You activate this protection function globally in the device.



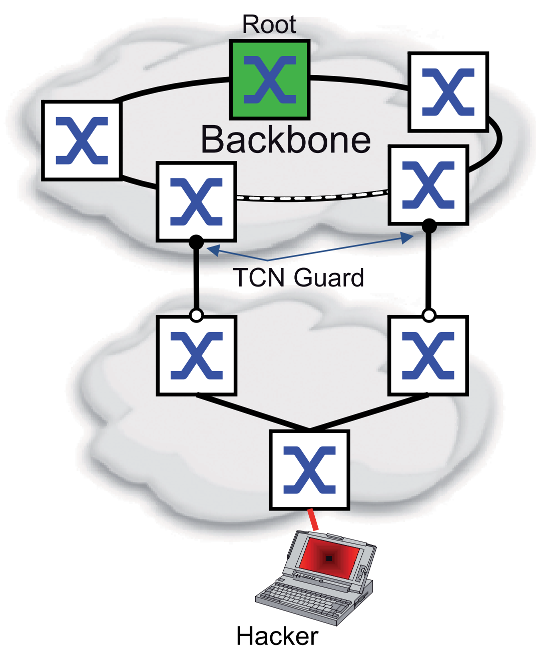
  Terminal device ports do not normally receive any STP-BPDUs. If an attacker still attempts to feed in STP-BPDUs at this port, the device deactivates the device port.

- Root Guard – for designated ports
  You activate this protection function separately for every device port.



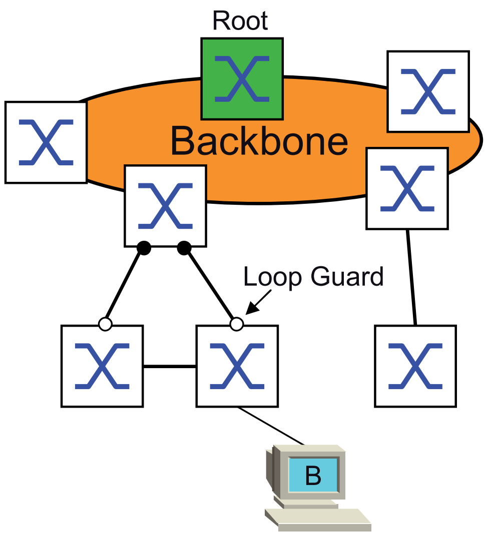
If a designated port receives an STP-BPDU with better path information to the root bridge, the device discards the STP-BPDU and sets the transmission state of the port to `discarding` instead of `root`.
If there are no STP-BPDUs with better path information to the root bridge, after 2 x `Hello Time` the device resets the state of the port to a value according to the port role.

- TCN Guard – for ports that receive STP-BPDUs with a Topology Change flag
  You activate this protection function separately for every device port.



If the protection function is activated, the device ignores Topology Change flags in received STP-BPDUs. This does not change the content of the address table (FDB) of the device port. However, additional information in the BPDU that changes the topology is processed by the device.

- Loop Guard – for root, alternate and backup ports
  You activate this protection function separately for every device port.



This protection function prevents the transmission status of a port from unintentionally being changed to `forwarding` if the port does not receive any more STP-BPDUs. If this situation occurs, the device designates the loop status of the port as inconsistent, but does not forward any data packets.

3.6.1 Activating the BPDU Guard

☐ Open the `Redundancy:Spanning Tree:Global` dialog.

☐ Select the "BPDU Guard" checkbox.

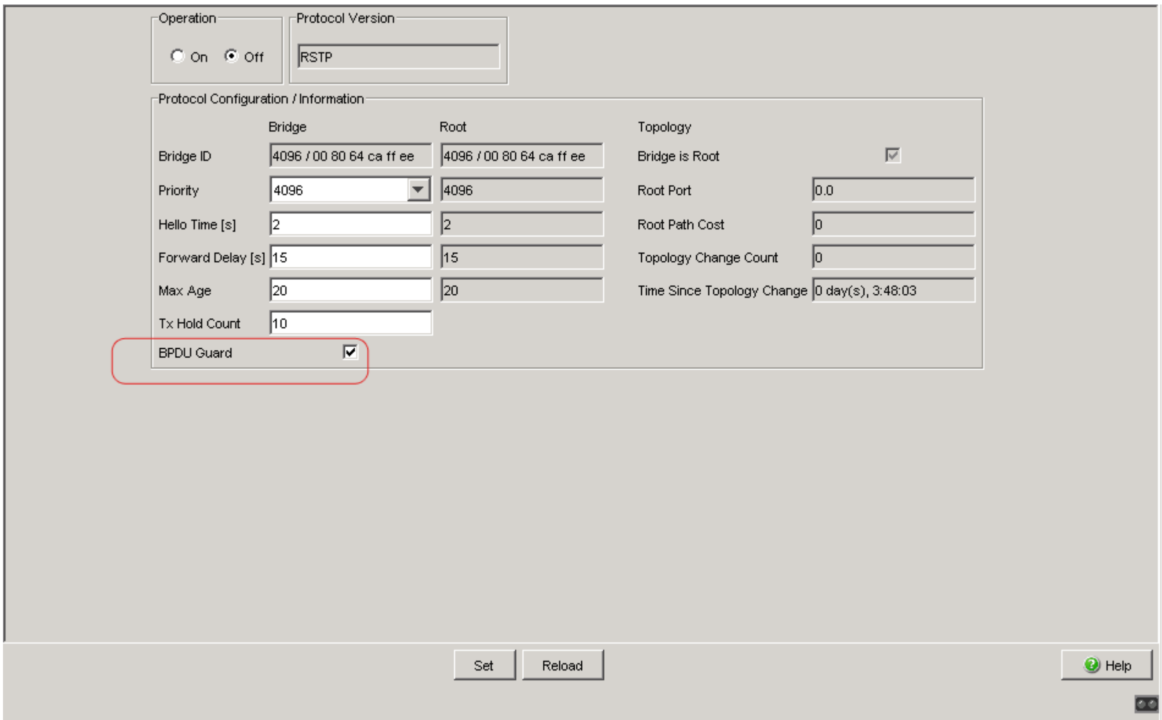


Figure 31: Activating the BPDU Guard

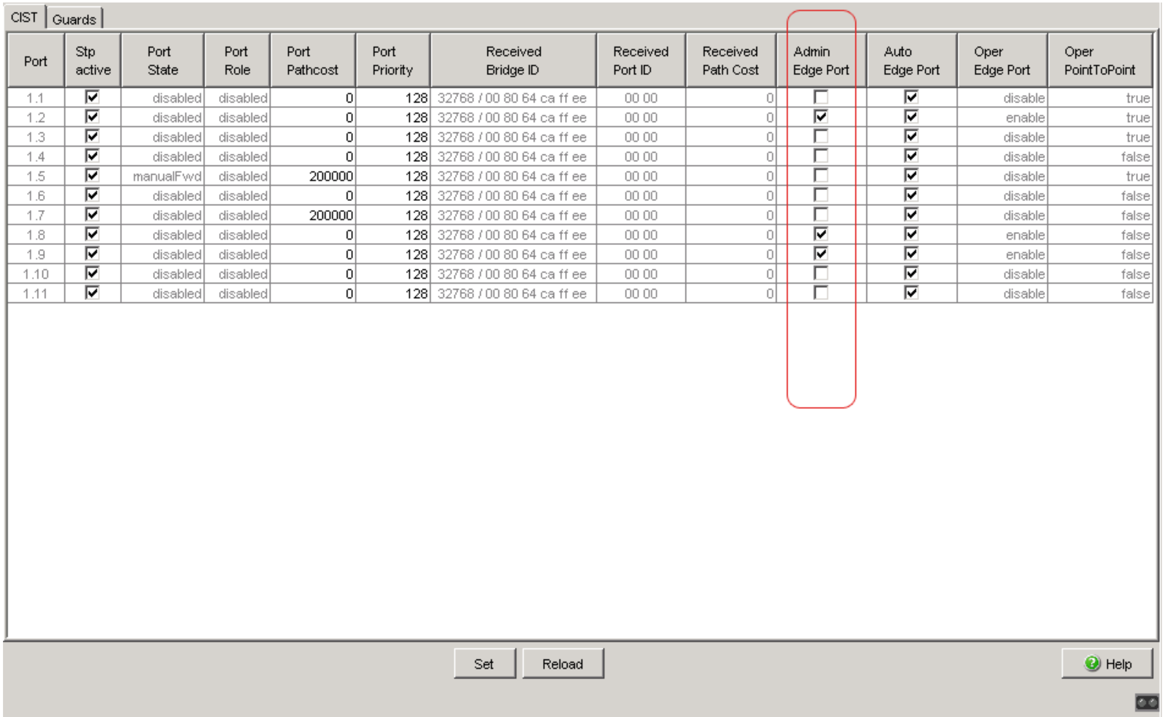
☐ Click on “Set” to save the changes.

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`spanning-tree bpdu-guard`	Activates the BPDU Guard.
`show spanning-tree global`	Displays the parameters for checking.

☐ Open the `Redundancy:Spanning Tree:Port` dialog.

☐ Switch to the "CIST" tab.

☐ For terminal device ports, select the checkbox in the "Admin Edge Port" column.



Port	Stp active	Port State	Port Role	Port Pathcost	Port Priority	Received Bridge ID	Received Port ID	Received Path Cost	Admin Edge Port	Auto Edge Port	Oper Edge Port	Oper PointToPoint
1.1	☑	disabled	disabled	0	128	32768 / 00 80 64 ca ff ee	00 00	0	☐	☑	disable	true
1.2	☑	disabled	disabled	0	128	32768 / 00 80 64 ca ff ee	00 00	0	☑	☑	enable	true
1.3	☑	disabled	disabled	0	128	32768 / 00 80 64 ca ff ee	00 00	0	☐	☑	disable	true
1.4	☑	disabled	disabled	0	128	32768 / 00 80 64 ca ff ee	00 00	0	☐	☑	disable	false
1.5	☑	manualFwd	disabled	200000	128	32768 / 00 80 64 ca ff ee	00 00	0	☐	☑	disable	true
1.6	☑	disabled	disabled	0	128	32768 / 00 80 64 ca ff ee	00 00	0	☐	☑	disable	false
1.7	☑	disabled	disabled	200000	128	32768 / 00 80 64 ca ff ee	00 00	0	☐	☑	disable	false
1.8	☑	disabled	disabled	0	128	32768 / 00 80 64 ca ff ee	00 00	0	☑	☑	enable	false
1.9	☑	disabled	disabled	0	128	32768 / 00 80 64 ca ff ee	00 00	0	☑	☑	enable	false
1.10	☑	disabled	disabled	0	128	32768 / 00 80 64 ca ff ee	00 00	0	☐	☑	disable	false
1.11	☑	disabled	disabled	0	128	32768 / 00 80 64 ca ff ee	00 00	0	☐	☑	disable	false

Figure 32: Port dialog, "CIST" tab

☐ Click on “Set” to save the changes.

`interface x/y`	Switches to the interface mode.
`spanning-tree edge-port`	Designates the port as a terminal device port (edge port).
`show spanning-tree port x/y`	Displays the parameters for checking.
`exit`	Leaves the interface mode.

If an edge port receives an STP-BPDU, the device behaves as follows:

- The device deactivates this port.
  In the `Basic Configuration:Port Configuration` dialog, the checkbox in the "Port on" column is not selected for this port.
- The device designates the port.

In the `Redundancy:Spanning Tree:Port` dialog, "CIST" tab, the device shows the value `enable` in the "BPDU Guard Effect" column.

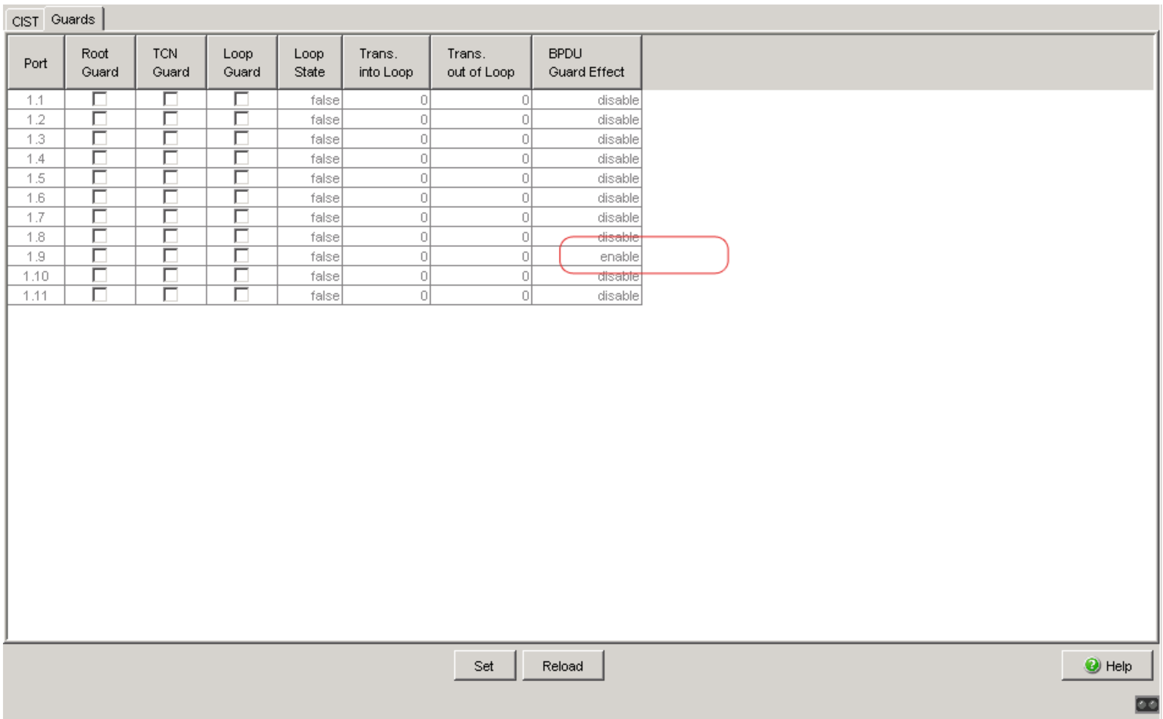


Figure 33: Port dialog, "Guards" tab

`show spanning-tree port x/y`	Displays the parameters of the port for checking. The value of the "BPDU Guard Effect" parameter is `enable`.

To reset the status of the device port to the value `forwarding`, you proceed as follows:

- ☐ If the device port is still receiving BPDUs:
  - – Remove the manual definition as an edge port.
    or
  - – Deactivate the BPDU Guard
- ☐ Activate the device port again.

3.6.2 Activating Root Guard / TCN Guard / Loop Guard

- ☐ Open the `Redundancy:Spanning Tree:Port` dialog.
- ☐ Switch to the "Guards" tab.
- ☐ For designated ports, select the checkbox in the "Root Guard" column.
- ☐ For ports that receive STP-BPDUs with a Topology Change flag, select the checkbox in the "TCN Guard" column.
- ☐ For root, alternate or backup ports, select the checkbox in the "Loop Guard" column.

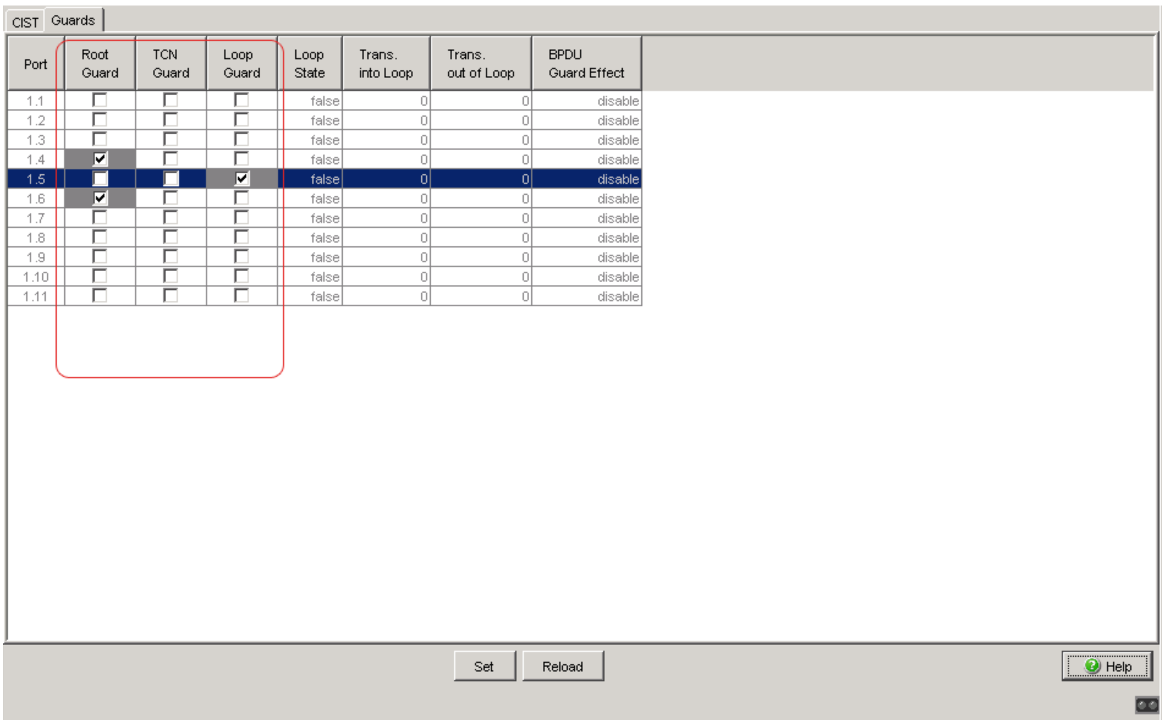


Figure 34: Activating Guards

Note: The `Root Guard` and `Loop Guard` functions are mutually exclusive. If you switch on the `Root Guard` function while the `Loop Guard` function is switched on, the device switches off the `Loop Guard` function.

- ☐ Click on “Set” to save the changes.

`enable`	Switch to the privileged EXEC mode.
`configure`	Switch to the Configuration mode.
`interface x/y`	Switches to the interface mode.
`spanning-tree guard-root`	Switches the Root Guard on at the designated port.
`spanning-tree guard-tcn`	Switches on the TCN Guard on the port that receives STP-BPDUs with a Topology Change flag.
`spanning-tree guard-loop`	Switches the Loop Guard on at a root, alternate or backup port.
`exit`	Leaves the interface mode.
`show spanning-tree port x/y`	Displays the parameters of the port for checking.

A Readers’ Comments

What is your opinion of this manual? We are always striving to provide as comprehensive a description of our product as possible, as well as important information that will ensure trouble-free operation. Your comments and suggestions help us to further improve the quality of our documentation.

Your assessment of this manual:

	Very good	Good	Satisfactory	Mediocre	Poor
Precise description	O	O	O	O	O
Readability	O	O	O	O	O
Understandability	O	O	O	O	O
Examples	O	O	O	O	O
Structure	O	O	O	O	O
Completeness	O	O	O	O	O
Graphics	O	O	O	O	O
Drawings	O	O	O	O	O
Tables	O	O	O	O	O

Did you discover any errors in this manual?
If so, on what page?

Suggestions for improvement and additional information:

General comments:

Sender:

Company / Department:

Name / Telephone no.:

Street:

Zip code / City:

e-mail:

Date / Signature:

Dear User,

Please fill out and return this page

- as a fax to the number +49 (0)7127 14-1600 or
- by post to

Hirschmann Automation and Control GmbH
Department 01RD-NT
Stuttgarter Str. 45-51
72654 Neckartenzlingen

B Index

C Further Support

■ Technical Questions

For technical questions, please contact any Hirschmann dealer in your area or Hirschmann directly.

You will find the addresses of our partners on the Internet at http://www.hirschmann.com

Contact our support at https://hirschmann-support.belden.eu.com

You can contact us

in the EMEA region at
- Tel.: +49 (0)1805 14-1538
- E-mail: hac.support@belden.com

in the America region at
- Tel.: +1 (717) 217-2270
- E-mail: inet-support.us@belden.com

in the Asia-Pacific region at
- Tel.: +65 6854 9860
- E-mail: inet-ap@belden.com

■ Hirschmann Competence Center

The Hirschmann Competence Center is ahead of its competitors:

- Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.
- Training offers you an introduction to the basics, product briefing and user training with certification.
  The current technology and product training courses can be found at http://www.hicomcenter.com
- Support ranges from the first installation through the standby service to maintenance concepts.

With the Hirschmann Competence Center, you have decided against making any compromises. Our client-customized package leaves you free to choose the service components you want to use.
Internet:
http://www.hicomcenter.com

HIRSCHMANN

A BELDEN BRAND